

第一章：对称与群

§1 平面的运动群

书后练习1.1. $P_4, Ex1$

证明：因为 O 是正交矩阵，且 $\det O = -1$ ，所以可设

$$O = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}.$$

显然， O 有特征值 ± 1 ，且在 $1 - \cos \theta \neq 0$ 时，属于特征值 1 的特征向量在直线

$$(1 - \cos \theta)x - \sin \theta y = 0$$

上。取直线 $l: (1 - \cos \theta)x - \sin \theta y = 0$ 。下面验证：

任意的 $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$ ，都有 $\begin{pmatrix} x \\ y \end{pmatrix}$ ， $O \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos \theta x + \sin \theta y \\ \sin \theta x - \cos \theta y \end{pmatrix}$ 关于直线 l 对称。

$\begin{pmatrix} x \\ y \end{pmatrix}$ 到直线 l 的距离是

$$\frac{|(1 - \cos \theta)x - \sin \theta y|}{\sqrt{2 - 2 \cos \theta}};$$

$O \begin{pmatrix} x \\ y \end{pmatrix}$ 到直线 l 的距离是

$$\left| \frac{(1 - \cos \theta)(\cos \theta x + \sin \theta y) - \sin \theta(\sin \theta x - \cos \theta y)}{\sqrt{2 - 2 \cos \theta}} \right| = \frac{|(1 - \cos \theta)x - \sin \theta y|}{\sqrt{2 - 2 \cos \theta}};$$

且 $\begin{pmatrix} x \\ y \end{pmatrix}$ 与 $O \begin{pmatrix} x \\ y \end{pmatrix}$ 的连线与 l 之间的斜率之积:

$$\frac{\sin \theta x - \cos \theta y - y}{\cos \theta x + \sin \theta y - x} \cdot \frac{1 - \cos \theta}{\sin \theta} = -1;$$

所以 $\begin{pmatrix} x \\ y \end{pmatrix}$ 与 $O \begin{pmatrix} x \\ y \end{pmatrix}$ 关于直线 l 对称. 这时, 运动 ϕ 是绕直线 l 的一个翻摺.

在 $1 - \cos \theta = 0$ 时, 属于特征值 1 的特征向量在直线

$$\sin \theta x - (1 + \cos \theta)y = 0$$

上. 取直线 $l_1: \sin \theta x - (1 + \cos \theta)y = 0$. 同样可以验证:

$\begin{pmatrix} x \\ y \end{pmatrix}$ 与 $O \begin{pmatrix} x \\ y \end{pmatrix}$ 关于直线 l_1 对称.

运动 ϕ 是绕直线 l_1 的一个翻摺. □

书后练习1.2. $P_4, Ex2$

证明: 任取 $\phi, \varphi, \theta \in T(M)$, 要验证 $(\phi \cdot \varphi) \cdot \theta = \phi \cdot (\varphi \cdot \theta)$, 只要验证: $\forall m \in M$, 都有

$$[(\phi \cdot \varphi) \cdot \theta](m) = [\phi \cdot (\varphi \cdot \theta)](m).$$

事实上, $[(\phi \cdot \varphi) \cdot \theta](m) = (\phi \cdot \varphi)(\theta m) = \phi[\varphi(\theta m)];$

$$[\phi \cdot (\varphi \cdot \theta)](m) = \phi[(\varphi \cdot \theta)(m)] = \phi[\varphi(\theta m)];$$

所以 $[(\phi \cdot \varphi) \cdot \theta](m) = [\phi \cdot (\varphi \cdot \theta)](m)$. 即 $(\phi \cdot \varphi) \cdot \theta = \phi \cdot (\varphi \cdot \theta)$. □

书后练习1.3. $P_4, Ex3$

解: $S(K)$ 是由: 恒等运动; 绕其中心转 60° ; 120° ; 180° ; 240° ; 300° 的旋转; 以及关于它的三条对角线; 三组对边中点的连线所作的翻摺. 一共是 12 个运动组成. □

§2 数域的对称

书后练习2.1. $P_8, Ex1$

证明: 显然 F 是含有 0, 1 的复数域 \mathbb{C} 的一个子集.

任意的 $a_i + b_i\sqrt{2} \in F$, $a_i, b_i \in \mathbb{Q}$, $i = 1, 2$, 都有:

$$(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2} \in F;$$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \in F;$$

$$\frac{1}{a_1 + b_1\sqrt{2}} = \frac{a_1}{a_1^2 - 2b_1^2} + \left(-\frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}\right) \in F.$$

即 F 对数的加法、减法和乘法是封闭的；且 $\forall 0 \neq a = a_1 + b_1\sqrt{2} \in F$, 都有 $a^{-1} = \frac{a_1}{a_1^2 - 2b_1^2} + \left(-\frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}\right) \in F$.

所以 F 是一个数域. □

书后练习2.2. $P_8, Ex2$

证明: 对任意的数域 F , 都有 $\mathbb{Q} \subset F$.

且显然有 $Aut(F : \mathbb{Q}) \subset Aut(F)$;

下只要证明: $Aut(F) \subset Aut(F : \mathbb{Q})$. 即数域 F 的任何一个自同构都保持 \mathbb{Q} 不变.

事实上: $\forall \phi \in Aut(F)$, 则 $\phi(1) = 1$, 从而对任意的正整数 n , $\phi(n) = n$, $\phi(-n) = -n$, $\phi(n^{-1}) = n^{-1}$; 所以对任意的 $q = \frac{m}{n} \in \mathbb{Q}$, $m, n \in \mathbb{Z}$, \mathbb{Z} 为整数集, 都有 $\phi(\frac{m}{n}) = \phi(m \cdot n^{-1}) = \phi(m) \cdot \phi(n^{-1}) = m \cdot n^{-1} = \frac{m}{n}$. 所以 $\phi \in Aut(F : \mathbb{Q})$. □

书后练习2.3. $P_8, Ex3$

证明: (1) 首先证明: 对任意的 $x, y \in \mathbb{Q}$, 若 $x + y\sqrt{2} = 0$, 则 $x = y = 0$.

对 $x, y \in \mathbb{Q}$ 不全为 0, 则存在 $z \in \mathbb{Q}$, 使得 zx, zy 都是整数, 且 $(zx, zy) = 1$. 不失一般性, 假设 x, y 是不全为 0 的整数且 $(x, y) = 1$.

由 $x + y\sqrt{2} = 0$ 可知: $x^2 = 2y^2$.

所以 x 是偶数, 可设 $x = 2k$, k 为整数. 从而 $2k^2 = y^2$, y 也是偶数. 这与 $(x, y) = 1$ 矛盾. 所以 $x = y = 0$.

(2) 同样可以证明: 对任意的 $x, y \in \mathbb{Q}$, 若 $x + y\sqrt{6} = 0$, 则 $x = y = 0$.

事实上: 只要证明对任意的整数 x, y , 若 $x + y\sqrt{6} = 0$, 则 $x = y = 0$. 不失一般性, 假设 x, y 是不全为 0 的整数且 $(x, y) = 1$.

由 $x + y\sqrt{6} = 0$ 可知: $x^2 = 6y^2$.

所以 x 是偶数, 可设 $x = 2k$, k 为整数. 从而 $2k^2 = 3y^2$, y 也是偶数. 这与 $(x, y) = 1$ 矛盾. 所以 $x = y = 0$.

(3) 同样可以证明: 对任意的 $x, y \in \mathbb{Q}$, 若 $x + y\sqrt{3} = 0$, 则 $x = y = 0$.

事实上: 只要证明对任意的整数 x, y , 若 $x + y\sqrt{3} = 0$, 则 $x = y = 0$.
不失一般性, 假设 x, y 是不全为 0 的整数且 $(x, y) = 1$.

由 $x + y\sqrt{3} = 0$ 可知: $x^2 = 3y^2$.

所以 x 是 3 的倍数, 可设 $x = 3k$, k 为整数. 从而 $3k^2 = y^2$, y 也是 3 的倍数. 这与 $(x, y) = 1$ 矛盾. 所以 $x = y = 0$.

(4) 再证明: 对任意的 $x, y, z \in \mathbb{Q}$, 若 $x + y\sqrt{2} + z\sqrt{3} = 0$, 则 $x = y = z = 0$.

由 $x + y\sqrt{2} + z\sqrt{3} = 0$ 可得

$$\begin{aligned}x^2 &= (y\sqrt{2} + z\sqrt{3})^2 = 2y^2 + 2yz\sqrt{6} + 3z^2, \\2y^2 + 3z^2 - x^2 + 2yz\sqrt{6} &= 0.\end{aligned}$$

由 (2) 的结论, 知 $yz = 0$, 即 $y = 0$ 或者 $z = 0$.

若 $y = 0$, 则 $x + y\sqrt{2} + z\sqrt{3} = 0 \Leftrightarrow x + z\sqrt{3} = 0$, 由 (3) 的结论, $x = z = 0$.

若 $z = 0$, 则 $x + y\sqrt{2} + z\sqrt{3} = 0 \Leftrightarrow x + y\sqrt{2} = 0$, 由 (1) 的结论, $x = y = 0$.

所以由 $x + y\sqrt{2} + z\sqrt{3} = 0$ 可得 $x = y = z = 0$.

(5) 再证明: 对任意的 $a, b, c, d \in \mathbb{Q}$, 若 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$, 则 $a = b = c = d = 0$.

由 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ 得

$$\begin{aligned}(b\sqrt{2} + c\sqrt{3} + d\sqrt{6})^2 &= (-a)^2, \\2b^2 + 3c^2 + 6d^2 + 4bd\sqrt{3} + 6dc\sqrt{2} &= a^2,\end{aligned}$$

所以由 (4) 的结论, 知 $bd = 0$ 且 $dc = 0$.

若 $d = 0$, 则 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \Leftrightarrow a + b\sqrt{2} + c\sqrt{3} = 0$, 由 (4) 的结论, $a = b = c = 0$;

若 $b = 0$ 且 $c = 0$, 则 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \Leftrightarrow a + d\sqrt{6} = 0$, 由 (2) 的结论, $a = d = 0$;

所以由 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$, 可得 $a = b = c = d = 0$. □

书后练习2.4. $P_8, Ex4$

证明: (1) 只要直接验证.

显然 $0, 1 \in \mathbb{Q}(i)$;

任意的 $a_k + b_k i \in \mathbb{Q}(i)$, $k = 1, 2$, 都有

$$(a_1 + b_1 i) \pm (a_2 + b_2 i) = (a_1 \pm a_2) + (b_1 \pm b_2)i \in \mathbb{Q}(i);$$

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i;$$

若 $0 \neq a_1 + b_1 i \in \mathbb{Q}(i)$, 则

$$(a_1 + b_1 i)^{-1} = \frac{a_1}{a_1^2 + b_1^2} + (-\frac{b_1}{a_1^2 + b_1^2})i \in \mathbb{Q}(i);$$

所以 $\mathbb{Q}(i)$ 是数域.

显然 $0, 1 \in \mathbb{Q}(i, \sqrt{5})$;

任意的 $a_k + b_k i + c_k \sqrt{5} + d_k \sqrt{5}i \in \mathbb{Q}(i)$, $k = 1, 2$, 都有

$$\begin{aligned} & (a_1 + b_1 i + c_1 \sqrt{5} + d_1 \sqrt{5}i) \pm (a_2 + b_2 i + c_2 \sqrt{5} + d_2 \sqrt{5}i) \\ &= (a_1 \pm a_2) + (b_1 \pm b_2)i + (c_1 \pm c_2)\sqrt{5} + (d_1 \pm d_2)\sqrt{5}i \in \mathbb{Q}(i, \sqrt{5}); \end{aligned}$$

$$\begin{aligned} & (a_1 + b_1 i + c_1 \sqrt{5} + d_1 \sqrt{5}i) \cdot (a_2 + b_2 i + c_2 \sqrt{5} + d_2 \sqrt{5}i) \\ &= (a_1 a_2 - b_1 b_2 + 5c_1 c_2 - 5d_1 d_2) + (a_1 b_2 + b_1 a_2 + 5c_1 d_2 + 5d_1 c_2)i \\ &+ (a_1 c_2 + c_1 a_2 - d_1 b_2 - b_1 d_2)\sqrt{5} + (a_1 d_2 + d_1 a_2 + c_1 b_2 + b_1 c_2)\sqrt{5}i \in \mathbb{Q}(i, \sqrt{5}); \end{aligned}$$

若 $0 \neq a + bi + c\sqrt{5} + d\sqrt{5}i \in \mathbb{Q}(i, \sqrt{5})$, 则

$$\begin{aligned} & (a + bi + c\sqrt{5} + d\sqrt{5}i)^{-1} \\ &= \frac{a(a^2+5c^2+b^2+5d^2)-5c(2ac+2bd)}{(a^2+5c^2+b^2+5d^2)^2-5(2ac+2bd)^2} + \frac{5d(2ac+2bd)-b(a^2+5c^2+b^2+5d^2)}{(a^2+5c^2+b^2+5d^2)^2-5(2ac+2bd)^2}i \\ &+ \frac{c(a^2+5c^2+b^2+5d^2)-a(2ac+2bd)}{(a^2+5c^2+b^2+5d^2)^2-5(2ac+2bd)^2}\sqrt{5} + \frac{d(a^2+5c^2+b^2+5d^2)+b(2ac+2bd)}{(a^2+5c^2+b^2+5d^2)^2-5(2ac+2bd)^2}\sqrt{5}i \in \mathbb{Q}(i, \sqrt{5}); \end{aligned}$$

所以 $\mathbb{Q}(i, \sqrt{5})$ 是数域.

(2) 由 $Ex2$ 知, $Aut(F : \mathbb{Q}) = Aut(F)$.

所以任意的 $\phi \in Aut(F)$, $a + bi \in \mathbb{Q}(i)$, 都有 $\phi(a + bi) = a + b\phi(i)$.

即 ϕ 完全被 $\phi(i)$ 所确定.

又因为 $i \cdot i = -1$, 所以 $\phi(i \cdot i) = \phi(-1) = -1$. 即 $\phi(i) \cdot \phi(i) = -1$, 所以 $\phi(i) = i$ 或者 $\phi(i) = -i$.

若 $\phi(i) = i$, 则

$$\begin{aligned} \phi : \mathbb{Q}(i) &\rightarrow \mathbb{Q}(i) \\ a + bi &\mapsto a + bi \end{aligned}$$

是 $\mathbb{Q}(i)$ 上的恒等映射.

若 $\phi(i) = -i$, 记

$$\begin{aligned}\phi_1 : \mathbb{Q}(i) &\rightarrow \mathbb{Q}(i) \\ a + bi &\mapsto a - bi\end{aligned}$$

是 $\mathbb{Q}(i)$ 上的自同构.

所以 $\text{Aut}(F)$ 中有两个元素, $\text{Aut}(\mathbb{Q}(i)) = \{I, \phi_1\}$, 其中 I 是 $\mathbb{Q}(i)$ 上的恒等映射.

由 Ex2 知, $\text{Aut}(E : \mathbb{Q}) = \text{Aut}(E)$.

所以任意的 $\phi \in \text{Aut}(E)$, $a + bi + c\sqrt{5} + d\sqrt{5}i \in \mathbb{Q}(i, \sqrt{5})$, 都有 $\phi(a + bi) = a + b\phi(i) + c\phi(\sqrt{5}) + d\phi(\sqrt{5})\phi(i)$.

即 ϕ 完全被 $\phi(i)$ 和 $\phi(\sqrt{5})$ 所确定.

又因为 $i \cdot i = -1$, 所以 $\phi(i \cdot i) = \phi(-1) = -1$. 即 $\phi(i) \cdot \phi(i) = -1$, 所以 $\phi(i) = i$ 或者 $\phi(i) = -i$.

而 $\sqrt{5} \cdot \sqrt{5} = 5$, 所以 $\phi(\sqrt{5} \cdot \sqrt{5}) = \phi(5) = 5$. 即 $\phi(\sqrt{5}) \cdot \phi(\sqrt{5}) = 5$, 所以 $\phi(\sqrt{5}) = \sqrt{5}$ 或者 $\phi(\sqrt{5}) = -\sqrt{5}$.

从而 $\text{Aut}(\mathbb{Q}(i, \sqrt{5}))$ 中可能有 4 个元素

$$\begin{aligned}I : \mathbb{Q}(i, \sqrt{5}) &\rightarrow \mathbb{Q}(i, \sqrt{5}) \\ a + bi + c\sqrt{5} + d\sqrt{5}i &\mapsto a + bi + c\sqrt{5} + d\sqrt{5}i; \\ \phi_1 : \mathbb{Q}(i, \sqrt{5}) &\rightarrow \mathbb{Q}(i, \sqrt{5}) \\ a + bi + c\sqrt{5} + d\sqrt{5}i &\mapsto a - bi + c\sqrt{5} - d\sqrt{5}i; \\ \phi_2 : \mathbb{Q}(i, \sqrt{5}) &\rightarrow \mathbb{Q}(i, \sqrt{5}) \\ a + bi + c\sqrt{5} + d\sqrt{5}i &\mapsto a + bi - c\sqrt{5} - d\sqrt{5}i; \\ \phi_3 : \mathbb{Q}(i, \sqrt{5}) &\rightarrow \mathbb{Q}(i, \sqrt{5}) \\ a + bi + c\sqrt{5} + d\sqrt{5}i &\mapsto a - bi - c\sqrt{5} + d\sqrt{5}i;\end{aligned}$$

且容易验证: $I, \phi_1, \phi_2, \phi_3 \in \text{Aut}(\mathbb{Q}(i, \sqrt{5}))$,

所以 $\text{Aut}(\mathbb{Q}(i, \sqrt{5})) = \{I, \phi_1, \phi_2, \phi_3\}$.

任意 $\phi \in \text{Aut}(E : F)$, 则 $\forall a \in \mathbb{Q}, \phi(a) = a$, $\phi(i) = i$, 且 $\text{Aut}(E : F) \subset \text{Aut}(E)$, 所以 $\text{Aut}(E : F)$ 中有两个元素 I, ϕ_2 , 即 $\text{Aut}(E : F) = \{I, \phi_2\}$. □

§3 多项式的对称

书后练习3.1. $P_{11}, Ex1$

解: $S_f = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$

□

书后练习3.2. $P_{11}, Ex2$

解: 含有 $x_1^3 x_2$ 的项数最小的对称多项式:

$$f(x_1, x_2, x_3) = x_1^3 x_2 + x_2^3 x_1 + x_1^3 x_3 + x_3^3 x_1 + x_2^3 x_3 + x_3^3 x_2$$

□

书后练习3.3. $P_{11}, Ex3$

证明: 在方程 $f(x, y) = 0$ 确定的图形 K 上任取一点 (a, b) , 则 $f(a, b) = 0$. 而 $f(x, y)$ 是对称多项式, 所以 $f(x, y) = f(y, x)$, 从而 $f(b, a) = 0$. 即如果点 (a, b) 在 K 上, 则其关于直线 $x - y = 0$ 的对称点 (b, a) 也在 K 上, 所以 K 关于直线 $x - y = 0$ 对称.

□

书后练习3.4. $P_{11}, Ex4$

证明: 显然 E 中含有 $\pm\sqrt{2}$, 包含多项式 $f = x^2 - 2$ 的全部根. E 是数域.

下面只要证明: E 是含有多项式 $f = x^2 - 2$ 的全部根的最小数域. 即: 如果数域 F 中含有 $\pm\sqrt{2}$, 则 $E \subset F$.

事实上: 由于 F 是数域, 所以有理数域 $\mathbb{Q} \subset F$. 而 $\sqrt{2} \in F$, 且 F 对数的运算封闭, 从而任意的 $a, b \in \mathbb{Q} \subset F$, $\sqrt{2} \in F$, 都有 $a + b\sqrt{2} \in F$, 所以 $E \subset F$. 所以 E 是包含 $\pm\sqrt{2}$ 的最小数域. 即 E 是多项式 $f = x^2 - 2$ 的分裂域.

□

第二章：群

§1 群

书后练习1.1. $P_{17}, Ex1$

证明：因为 (G, \cdot) 是群，所以对任意的 $a \in G$ ，存在 $x \in G$ ，使得

$$ax = xa = e,$$

其中 e 为 (G, \cdot) 的单位元.

所以在 G 中，

$$ab = ac \Rightarrow x(ab) = x(ac) \Rightarrow (xa)b = (xa)c \Rightarrow eb = ec \Rightarrow b = c;$$

$$ba = ca \Rightarrow (ba)x = (ca)x \Rightarrow b(ax) = c(ax) \Rightarrow be = ce \Rightarrow b = c;$$

即 (G, \cdot) 满足消去律. □

书后练习1.2. $P_{17}, Ex2$

证明：(1) 因为 (S, \cdot) 是半群，任取 $x \in S$ ，由于 $xS = S$ ，所以存在 $e_1 \in S$ ，使得 $xe_1 = x$ ；对任意的 $y \in G$ ，由于 $Sy = S$ ，所以存在 $z \in G$ ，使得 $zx = y$ ；所以

$$ye_1 = (zx)e_1 = z(xe_1) = zx = y;$$

同样，任取 $x \in S$ ，由于 $Sx = S$ ，所以存在 $e_2 \in S$ ，使得 $e_2x = x$ ；对任意的 $y \in G$ ，由于 $yS = S$ ，所以存在 $z \in G$ ，使得 $xz = y$ ；所以

$$e_2y = e_2(xz) = (e_2x)z = xz = y;$$

所以 $e_1 = e_2e_1 = e_2 = e$ 是 (S, \cdot) 的单位元，

任意的 $y \in S$, 因为 $yS = Sy = S$, 所以存在 $y_1, y_2 \in S$, 使得

$$xy_1 = y_2x = e,$$

从而

$$y_1 = ey_1 = (y_2x)y_1 = y_2(xy_1) = y_2e = y_2,$$

即 $y_1 = y_2$ 是 y 的逆元.

所以 (S, \cdot) 是一个群.

(2) 因为 (S, \cdot) 是一个有限半群, 且满足消去律, 所以对任意的 $a \in S$, 作

$$f_a : S \rightarrow S, x \mapsto ax,$$

则 f_a 是 S 到 S 的一个映射, 且 $f_a(S) = aS$. 对任意的 $x, y \in S$, 若 $f_a(x) = f_a(y)$, 即 $ax = ay$, 由消去律, $x = y$. 所以 f_a 是 S 到 S 的单射. 注意到 S 是有限集, 所以 f_a 是满射, 从而 $aS = S$.

同样作

$$g_a : S \rightarrow S, x \mapsto xa,$$

则 g_a 是 S 到 S 的一个映射, 且 $g_a(S) = Sa$. 对任意的 $x, y \in S$, 若 $g_a(x) = g_a(y)$, 即 $xa = ya$, 由消去律, $x = y$. 所以 g_a 是 S 到 S 的单射. 注意到 S 是有限集, 所以 g_a 是满射, 从而 $Sa = S$.

由 (1), (S, \cdot) 是一个群.

(有限集合 A 上的单射一定是满射)

□

书后练习1.3. $P_{17}, Ex3$

证明: 首先 ϕ^{-1} 是 H 到 G 的一个一一对应. 且任意的 $x, y \in H$, 存在 $a, b \in G$, 使得

$$\begin{aligned}\phi(a) &= x, \phi(b) = y, \phi(a \cdot b) = \phi(a) \times \phi(b) = x \times y; \\ \phi^{-1}(x) &= a, \phi^{-1}(y) = b, \phi^{-1}(x \times y) = a \cdot b = \phi^{-1}(x) \cdot \phi^{-1}(y);\end{aligned}$$

所以 ϕ^{-1} 是 (H, \times) 到 (G, \cdot) 的一个同构对应.

□

书后练习1.4. $P_{17}, Ex4$

证明: (1) 直接验证: (\mathbb{Z}, \oplus) 构成一个交换群.

(i) 运算 \oplus 显然是封闭的;

- (ii) 结合律成立;
- (iii) 有单位元 1. 任意的 $a \in \mathbb{Z}$, $a \oplus 1 = a + 1 - 1 = a = 1 \oplus a$;
- (iv) 每一个元都有逆元. 任意的 $a \in \mathbb{Z}$, 存在 $-a + 2 \in \mathbb{Z}$, 使得 $a \oplus (-a + 2) = a + (-a + 2) - 1 = 1 = (-a + 2) \oplus a$;
- (v) 交换律成立.

所以 (\mathbb{Z}, \oplus) 是一个交换群.

(2) ϕ 显然是 \mathbb{Z} 到 \mathbb{Z} 的一个一一对应. 且任意的 $a, b \in \mathbb{Z}$, $\phi(a + b) = a + b + 1 = (a + 1) + (b + 1) - 1 = (a + 1) \oplus (b + 1) = \phi(a) \oplus \phi(b)$;

所以 ϕ 是 $(\mathbb{Z}, +)$ 到 (\mathbb{Z}, \oplus) 的群同构. \square

§2 子群

书后练习2.1. $P_{22}, Ex1$

证明: 作带余除法: 对整数 m 和自然数 n , 存在整数 l 和自然数 $0 \leq r < n$, 使得

$$m = ln + r,$$

$$a^m = a^{ln+r} = a^{nl}a^r = (a^n)^la^r, \text{ 所以 } a^r = e;$$

由 n 的最小性, 知 $r = 0$, 所以 $n|m$. \square

书后练习2.2. $P_{22}, Ex2$

证明: 若 ab, ba 都是无穷阶的, 结论显然成立.

假设 ab, ba 至少有一个的阶为有限. 不妨设 ab 是有限阶, 阶数为 n , 即 $(ab)^n = e$, e 是 G 的单位元. 则

$$(ba)^{n+1} = b(ab)^na = bea = ba \Rightarrow (ba)^n = e,$$

所以 ba 也是有限阶的. 设 ba 的阶数为 m , 由 $(ba)^n = e$ 以及 $Ex1$ 的结论, 则 $m|n$;

同样由 $(ba)^m = e$, 则

$$(ab)^{m+1} = a(ba)^mb = aeb = ab \Rightarrow (ab)^m = e,$$

由 ab 的阶为 n 以及 $Ex1$ 的结论, 则 $n|m$.

所以 $m=n$. ab 与 ba 有相同的阶. □

书后练习2.3. $P_{22}, Ex3$

证明: (1) 因为 H, K 是 G 的子群, 所以

$$H^{-1} = H, K^{-1} = K, HH = H, KK = K, (HK)^{-1} = K^{-1}H^{-1} = KH.$$

若 HK 是 G 的子群, 则

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH;$$

若 $HK = KH$, 则

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK,$$

HK 对 G 的运算封闭;

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK,$$

HK 中每一个元素的逆元也在 HK 中;

所以 HK 是 G 的一个子群.

(2) 因为 H 是 G 的正规子群, 所以对任意的 $a \in G$, 都有 $aH = Ha$, 从而对 G 的子群 K , 都有 $HK = KH$, 利用 (1) 的结论, 有 HK 是 G 的子群. □

书后练习2.4. $P_{22}, Ex4$

解: $S_3 = \{I, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}.$

它有一个一阶子群: $G_1 = \{I\};$

三个二阶子群:

$$G_2 = \{I, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\}, G_3 = \{I, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}, G_4 = \{I, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\};$$

$$\text{一个三阶子群: } G_5 = \{I, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\};$$

一个六阶子群: S_3 自身.

其中, G_2, G_3, G_4, G_5 是 G 的非平凡子群.

G_5 是 S_3 的正规子群. □

书后练习2.5. P_{22} , Ex5

证明: 要证明 G 的内自同构群 $\text{Inn}(G)$ 是自同构群 $\text{Aut}(G)$ 的正规子群, 只要证明, 任意的 $T_a \in \text{Inn}(G)$ 以及任意的 $\sigma \in \text{Aut}(G)$, 都有 $\sigma T_a \sigma^{-1} \in \text{Inn}(G)$.

事实上: $\forall x \in G$,
 $(\sigma T_a \sigma^{-1})x = \sigma(T_a(\sigma^{-1}x)) = \sigma(a(\sigma^{-1}x)a^{-1}) = \sigma(a)\sigma(\sigma^{-1}x)\sigma(a^{-1})$
 $= (\sigma a)x(\sigma a)^{-1} = T_{\sigma a} \in \text{Inn}(G)$.

所以 $\text{Inn}(G)$ 是 $\text{Aut}(G)$ 的一个正规子群. \square

§3 生成元集, 循环群

书后练习3.1. P_{27} , Ex1

解: $i^{-1} = (i_l i_{l-1} \cdots i_2 i_1)$. i 的阶为 t .

一般的, m -循环的阶为 m . \square

书后练习3.2. P_{27} , Ex2

证明: 设 $G = \langle a \rangle$ 是一个循环群. H 是 G 的一个子群.

如果 $H = \{e\} = \langle e \rangle$, 结论显然成立.

假设 $H \neq \{e\}$, 则存在 $e \neq b \in G$, 由于 $G = \langle a \rangle$, 所以存在 $l \in \mathbb{Z}$, 使得 $b = a^l$, 又 H 是群, 所以 $a^{-l} = b^{-1} \in H$. 记 $M = \{k | a^k \in H, k \in \mathbb{N}^+\}$, 则 $M \neq \emptyset$. 取 $m = \min M$, 则 $H = \langle a^m \rangle$.

事实上, $\forall h \in H$, 存在 $k \in \mathbb{Z}$, 使得 $h = a^k$. 作整数的带余除法, 则存在 $q, r \in \mathbb{Z}, 0 \leq r < m$, 使得

$$k = qm + r,$$

从而

$$a^k = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r,$$
$$a^r = a^k (a^m)^{-q}.$$

又因为 H 是群, $a^k \in H, a^m \in H, (a^m)^{-q} \in H$, 所以 $a^r \in H$, 再由 m 的取法知道, $r = 0$. 所以 $h = a^k = (a^m)^q$, 从而 $H = \langle a^m \rangle$ 是循环群. \square

书后练习3.3. P_{27} , Ex3

证明: 1) 首先由群中元素的阶的定义, 任意知道下列事实:

设 G 是一个群, m 是一个正整数, $a \in G$ 满足 $a^m = e$, 那么 a 是 G 的 m 阶元当且仅当对整数 n , 若 $a^n = e$, 则必有 $m \mid n$.

因为 $(a^s)^{\frac{n}{(s,n)}} = (a^n)^{\frac{s}{(s,n)}} = e^{\frac{s}{(s,n)}} = e$; 且任意的 $k \in \mathbb{Z}$, 若 $(a^s)^k = e = a^{sk}$, 则由 a 的阶为 n 知: $n \mid (sk)$, 从而 $\frac{n}{(s,n)} \mid \frac{s}{(s,n)}k$, 注意到 $(\frac{n}{(s,n)}, \frac{s}{(s,n)}) = 1$, 所以 $\frac{n}{(s,n)} \mid k$, 从而 a^s 的阶为 $\frac{n}{(s,n)}$.

2) 利用 1) 的结论, 元素 $a^{(s,n)}$ 的阶为 $\frac{n}{((s,n),n)} = \frac{n}{(s,n)}$, 所以 a^s 与 $a^{(s,n)}$ 有相同的阶.

3) 首先 $\langle a^s \rangle$ 与 $\langle a^{(s,n)} \rangle$ 都是 $\frac{n}{(s,n)}$ 阶循环群. 且存在 $l, k \in \mathbb{Z}$, 使得 $(s, n) = ls + kn$, 所以

$$a^{(s,n)} = a^{ls+kn} = (a^s)^l (a^n)^k = (a^s)^l \in \langle a^s \rangle,$$

所以 $\langle a^{(s,n)} \rangle \subseteq \langle a^s \rangle$, 从而 $\langle a^{(s,n)} \rangle = \langle a^s \rangle$. □

书后练习3.4. $P_{27}, Ex4$

解: 群 G 中有六个元素 $G = \{e, a, b, b^2, ab, ba\}$, 它的乘法表为:

\cdot		e	a	b	b^2	ab	ba
$-$		$-$	$-$	$-$	$-$	$-$	$-$
e		e	a	b	b^2	ab	ba
a		a	e	ab	ba	b	b^2
b		b	ba	b^2	e	a	ab
b^2		b^2	ab	e	b	ba	a
ab		ab	b^2	ba	a	e	b
ba		ba	b	a	ab	b^2	e

□

书后练习3.5. $P_{27}, Ex5$

证明: 1) 由于任何一个都可以表成不相交循环的乘积, 而任何一个 t -循环都可以表成若干对换的乘积, 所以只要证明: 任意一个对换都可以表成一些相邻对换的乘积. 设 $(i\ j), i < j$ 是任意一个对换, 我们对 $j - i$ 进行数学归纳:

$j - i = 1$, 结论显然成立.

假设 $j - i = m$ 成立, 则当 $j - i = m + 1$ 时, 则 $(i j) = (i i + 1)(i + 1 j)(i i + 1)$, 再利用归纳假设, $(i + 1 j)$ 可以表成一些相邻对换的乘积, 从而 $(i j)$ 可以表成一些相邻对换的乘积.

2) 因为任何一个相邻对换 $(i i + 1) = (1 i)(1 i + 1)(1 i)$, 所以 $\{(1 2), (1 3), \dots, (1 n)\}$ 是 S_n 的一个生成元集.

3) 因为所有的 3- 循环是 A_n 生成元集, 所以只要证明: 任何一个 3- 循环都可以表成 $(1 2 i)$ 这类 3- 循环的乘积. 事实上:

$$(i j k) = (1 2 k)(1 2 j)(1 2 i)(1 2 k)(1 2 j), i, j, k \neq 1, 2;$$

$$(1 i j) = (1 2 i)(1 2 j)(1 2 j)(1 2 i)(1 2 i), i, j \neq 1, 2;$$

$$(2 1 i) = (1 2 i)(1 2 i), i \neq 1, 2;$$

$$(2 i j) = (1 2 i)(1 2 j)(1 2 j), i, j, k \neq 1, 2.$$

所以 $\{(1 2 3), (1 2 4), \dots, (1 2 n)\}$ 是 A_n 的一个生成元集. □

§4 子群 (续)

书后练习4.1. $P_{32}, Ex1$

证明: 取 $b = a^{\frac{n}{2}}$, 则 $b \neq e, b^2 = e$, 且 G 中的 2 阶元是唯一的.

任意的 $f \in \text{Aut}(G)$, 则 $(f(b))^2 = f(b^2) = f(e) = e$,

所以 $f(b) = a^{\frac{n}{2}} = b$, b 是 $\text{Aut}(G)$ 的一个不动点. □

书后练习4.2. $P_{32}, Ex2$

解: $B_4 \cong \{T_e, T_a, T_b, T_c\}$.

$$T_e = (e), T_a = (e a)(b c), T_b = (e b)(a c), T_c = (e c)(a b). \quad \square$$

§5 商群

书后练习5.1. $P_{37}, Ex1$

证明: 因为 $\psi = \{[a] | a \in G\}$ 是群 G 的一个合同划分, 所以对任意的 $a, b \in G$, 都有

$$[a][b] \subseteq [ab];$$

而

$$[ab] = ab[e] \subseteq a[b][e] \subseteq a[be] = a[b] \subseteq [a][b];$$

所以

$$[a][b] = [ab].$$

□

书后练习5.2. $P_{37}, Ex2$

证明: 1) 设 \sim 是 G 的一个等价关系, 要证明: H 是 G 的一个子群.

取 $x \in G$, 则 $x \sim x$, 从而 $xx^{-1} = e \in H$, H 中有 G 的单位元, $H \neq \emptyset$;

任意的 $x, y \in H$, 由于 $xe^{-1} = x \in H, ye^{-1} = y \in H$, 所以 $x \sim e \sim y$, 从而 $x \sim y, xy^{-1} \in H$.

任意的 $y \in H, y^{-1} = ey^{-1} \in H$. H 中每一个元素的逆元都在 H 中;

任意的 $x, y \in H, y^{-1} \in H, xy = x(y^{-1})^{-1} \in H$, H 对 G 的运算封闭.

所以 H 是 G 的子群.

假设 H 是 G 的一个子群, 要证明 \sim 是 G 的一个等价关系.

任意的 $x \in G$, 则 $xx^{-1} = e \in H, x \sim x$, \sim 具有反身性;

任意的 $x, y \in G$, 若 $x \sim y$, 则 $xy^{-1} \in H, yx^{-1} = (xy^{-1})^{-1} \in H$, 所以 $y \sim x$, \sim 具有对称性;

任意的 $x, y, z \in G$, 若 $x \sim y, y \sim z$, 则 $xy^{-1}, yz^{-1} \in H, xz^{-1} = (xy^{-1})(yz^{-1}) \in H, x \sim z$, \sim 具有传递性.

所以 \sim 是 G 的一个等价关系.

2) 设 \sim 是 G 的一个合同关系, 要证明: H 是 G 的一个正规子群.

由 \sim 是 G 的一个合同关系, 则 \sim 是 G 的等价关系, 从而 H 是 G 的子群.

对任意的 $a \in G, x \in H$, 则 $a \sim a, x \sim e$, 所以 $ax \sim ae, ax \sim a, axa^{-1} \in H$, 从而 $aHa^{-1} \subseteq H$, H 是 G 的正规子群;

假设 H 是 G 的一个正规子群, 要证明 \sim 是 G 的一个合同关系.

由于假设 H 是 G 的一个子群, 所以 \sim 是 G 的一个等价关系. 设任意的 $a, b, c, d \in G$, $a \sim b$, $c \sim d$, $ab^{-1}, cd^{-1} \in H$, 注意到 H 是 G 的正规子群, 所以 $a(cd^{-1})a^{-1} \in H$, 从而

$$a(cd^{-1})a^{-1}(ab^{-1}) = a(cd^{-1})b^{-1} = ac(d^{-1}b^{-1}) = ac(bd)^{-1} \in H,$$

所以 $ac \sim bd$, 从而 \sim 是 G 的一个合同关系. \square

书后练习5.3. $P_{37}, Ex3$

证明: 1) 首先证明: ψ 是一个划分.

任意的 $x \in \mathbb{R}$, 显然 $x \in [x]$, $\blacksquare = \bigcup_{x \in \mathbb{R}} [x]$;

任意的 $x, y \in \mathbb{R}$, 若 $[x] \cap [y] \neq \emptyset$, 则存在 $z \in [x] \cap [y]$, 使得 $z = n_1a + x = n_2a + y$, 这时, 任意的 $r \in [x]$,

$$\begin{aligned} r &= na + x = (n - n_1)a + n_1a + x \\ &= (n - n_1)a + n_2a + y = (n - n_1 + n_2)a + y \in [y], \end{aligned}$$

$[x] \subseteq [y]$; 任意的 $r \in [y]$,

$$\begin{aligned} r &= na + y = (n - n_2)a + n_2a + y \\ &= (n - n_2)a + n_1a + x = (n - n_2 + n_1)a + x \in [x], \end{aligned}$$

$[y] \subseteq [x]$;

所以 $[x] = [y]$. 所以 ψ 是 \mathbb{R} 的一个划分.

下面证明: ψ 是 \mathbb{R} 的合同划分.

任意的 $[x], [y] \in \psi$, $[x] + [y] = \{n_1a + x + n_1a + y\} = [x + y]$, 所以 ψ 是 \blacksquare 的合同划分.

2) 首先 $C = \{e^{i\theta} | 0 \leq \theta < 2\pi\}$, 且任意的 $x \in \mathbb{R}$,

$$\phi([x]) = e^{i\frac{2\pi}{a}x}.$$

ϕ 是良定的. 即: 若 $[x] = [y]$, 则 $\phi([x]) = \phi([y])$.

事实上: $[x] = [y] \Leftrightarrow x - y = na$, 从而

$$\phi([x]) = e^{i\frac{2\pi}{a}x} = e^{i\frac{2\pi}{a}(na+y)} = e^{i2\pi n} e^{i\frac{2\pi}{a}y} = e^{i\frac{2\pi}{a}y} = \phi([y]);$$

ϕ 是单射.

事实上: 如果 $\phi([x]) = \phi([y])$, 即 $e^{i\frac{2\pi}{a}x} = e^{i\frac{2\pi}{a}y}$. 所以 $e^{i\frac{2\pi}{a}(x-y)} = 1$. 从而 $\frac{2(x-y)\pi}{a} = 2n\pi$, $x - y = na$, $[x] = [y]$;

ϕ 是满射.

事实上: 任意的 $e^{i\theta} \in C$, 存在 $x = \frac{a}{2\pi}\theta \in \mathbb{R}$, $[\frac{a}{2\pi}\theta] \in \psi$,
 $\phi([\frac{a}{2\pi}\theta]) = e^{i\frac{2\pi}{a}\frac{a}{2\pi}\theta} = e^{i\theta}$;

ϕ 保持运算.

事实上: 任意的 $[x], [y] \in \psi$, $\phi([x]) = e^{i\frac{2\pi}{a}x}$, $\phi([y]) = e^{i\frac{2\pi}{a}y}$,
 $\phi([x] + [y]) = e^{i\frac{2\pi}{a}(x+y)} = e^{i\frac{2\pi}{a}x}e^{i\frac{2\pi}{a}y} = \phi([x])\phi([y])$;

所以, ϕ 是 $(\psi, +)$ 到 (C, \cdot) 的一个同构. □

§6 同态

书后练习6.1. P_{42} , Ex1

证明: 1) 任意的 $a, b \in \phi(S)$, 则存在 $x, y \in S$, 使得 $\phi(x) = a$, $\phi(y) = b$, $xy \in S$, 所以

$$ab = \phi(x)\phi(y) = \phi(xy) \in \phi(S),$$

$\phi(S)$ 对乘法封闭;

任意的 $a \in \phi(S)$, 则存在 $x \in S$, 使得 $\phi(x) = a$, 又因为 S 是群, 所以 $x^{-1} \in S$, $\phi(x^{-1}) \in \phi(S)$, 即有

$$a^{-1} = (\phi(x))^{-1} = \phi(x^{-1}) \in \phi(S),$$

$\phi(S)$ 中每一个元都有逆元.

而 $\phi(S) \subseteq H$, 所以 $\phi(S)$ 是 H 的子群.

2) 任意的 $x, y \in \phi^{-1}(T)$, 则 $\phi(x), \phi(y) \in T$, 注意到 T 是 H 的一个子群, 所以

$$\phi(x^{-1}) = (\phi(x))^{-1} \in T, \quad x^{-1} \in \phi^{-1}(T),$$

$\phi^{-1}(T)$ 中每一个元素的逆元仍在 $\phi^{-1}(T)$; 且

$$\phi(xy) = \phi(x)\phi(y) \in T, \quad xy \in \phi^{-1}(T),$$

$\phi^{-1}(T)$ 关于 G 的乘法封闭.

所以, $\phi^{-1}(T)$ 是 G 的一个子群. 再

假设 T 是 H 的正规子群, 则对任意的 $h \in H, t \in T$, 都有

$$hth^{-1} \in T, \text{ 亦即 } hTh^{-1} \subseteq T.$$

任意的 $a \in G, b \in \phi^{-1}(T)$, 则 $\phi(a) \in H, \phi(b) \in T, \phi(a^{-1}) \in H$, 从而

$$\begin{aligned}\phi(aba^{-1}) &= \phi(a)\phi(b)\phi(a^{-1}) \in T, \\ aba^{-1} &\in \phi^{-1}(T),\end{aligned}$$

所以 $\phi^{-1}(T)$ 是 G 的正规子群.

3) 任意的 $a \in S \cdot \text{Ker}\phi$, 存在 $x \in S, y \in \text{Ker}\phi, a = xy$,

$$\begin{aligned}\phi(a) &= \phi(xy) = \phi(x)\phi(y) = \phi(x)e = \phi(x) \in \phi(S), \\ a &\in \phi^{-1}(\phi(S)),\end{aligned}$$

$$S \cdot \text{Ker}\phi \subseteq \phi^{-1}(\phi(S));$$

任意的 $b \in \phi^{-1}(\phi(S))$, 则存在 $\phi(b) \in \phi(S)$, 从而存在 $s \in S$, 使得 $\phi(b) = \phi(s)$. 从而

$$\begin{aligned}\phi(s^{-1}b) &= \phi(s^{-1})\phi(b) = (\phi(s))^{-1}\phi(b) = (\phi(b))^{-1}\phi(b) = e, \\ s^{-1}b &\in \text{Ker}\phi, b = s(s^{-1}b) \in S \cdot \text{Ker}\phi;\end{aligned}$$

$$\phi^{-1}(\phi(S)) \subseteq S \cdot \text{Ker}\phi;$$

所以, $\phi^{-1}(\phi(S)) = S \cdot \text{Ker}\phi$. □

书后练习6.2. $P_{42}, Ex2$

证明: 首先证明: θ 是 $L(G, H)$ 到 $L(\overline{G})$ 的一个一一对应.

θ 是映射;

事实上: 只要说明 S 是 G 的子群, 则 $\phi(S)$ 是 \overline{G} 的子群.

θ 是单射;

事实上: 假设 $S_1, S_2 \in L(G, H)$, 且 $\theta(S_1) = \theta(S_2), \phi(S_1) = \phi(S_2)$, 要证明: $S_1 = S_2$.

任意的 $x \in S_1$, 则 $\phi(x) \in \phi(S_1) = \phi(S_2)$, 所以存在 $y \in S_2$, 使得 $\phi(y) = \phi(x)$, 从而 $\phi(xy^{-1}) = e$, $xy^{-1} = s \in \text{Ker}\phi = H \subseteq S_2$, 所以 $x = ys \in S_2, S_1 \subseteq S_2$;

同理可以证明: $S_2 \subseteq S_1$;

θ 是满射;

事实上: 任意的 $\overline{S} \in L(\overline{G})$, 则 $\phi^{-1}(\overline{S}) \in L(G, H)$, 满足:

$$\theta(\phi^{-1}(\overline{S})) = \phi(\phi^{-1}(\overline{S})) = \overline{S}.$$

1) 设 $S, T \in L(G, H)$, $S \supseteq T (\supseteq H = \text{Ker}\phi)$. 任意的 $x \in \phi(T)$, 存在 $y \in T \subseteq S$, 使得 $\phi(y) = x \in \phi(S)$, 所以 $\phi(T) \subseteq \phi(S)$;

假设 $\phi(T) \subseteq \phi(S)$. 任意的 $x \in T$, $\phi(x) \in \phi(T) \subseteq \phi(S)$, 所以存在 $y \in S$, 使得 $\phi(y) = \phi(x)$, $\phi(xy^{-1}) = e$, $xy^{-1} \in \text{Ker}\phi = H \subseteq S$, 所以存在 $h \in H$, 使得 $xy^{-1} = h$, $x = hy \in S$, $T \subseteq S$.

2) 假设 S 是 G 的正规子群, 则 S 是 G 的子群, $\phi(S)$ 是 \bar{G} 的子群. 任意的 $x \in \phi(S)$, $y \in \bar{G}$, 则存在 $a \in S$, $b \in G$, 使得 $\phi(a) = x$, $\phi(b) = y$, $\phi(b^{-1}) = y^{-1}$, 而 S 是正规子群, 所以 $bab^{-1} \in S$, 从而:

$$yxy^{-1} = \phi(b)\phi(a)\phi(b^{-1}) = \phi(bab^{-1}) \in \phi(S),$$

所以 $\phi(S)$ 是 \bar{G} 的正规子群.

假设 $\phi(S)$ 是 \bar{G} 的正规子群, 则对任意的 $x \in \phi(S)$, $y \in \bar{G}$, 都有 $yxy^{-1} \in \phi(S)$.

任意的 $a \in S, b \in G$, 则 $\phi(a) \in \phi(S)$, $\phi(b), \phi(b^{-1}) \in \bar{G}$, $\phi(bab^{-1}) = \phi(b)\phi(a)\phi(b^{-1}) = \phi(b)\phi(a)(\phi(b))^{-1} \in \phi(S)$, 所以存在 $s \in S$, 使得 $\phi(bab^{-1}) = \phi(s)$, $\phi(bab^{-1}s^{-1}) = e$, $bab^{-1}s^{-1} \in \text{Ker}\phi \subseteq H \subseteq S$, 所以存在 $h \in H$, 使得 $bab^{-1}s^{-1} = h$. $bab^{-1} = hs \in S$. 所以 S 是 G 的正规子群.

3) 假设 S 是 G 的正规子群, 则 $\phi(S)$ 是 \bar{G} 的正规子群. 所以 $\bar{G}/\phi(S)$ 是的商群. 作:

$$\begin{aligned}\sigma: G &\rightarrow \bar{G}/\phi(S), \\ x &\mapsto [\phi(x)] = \phi(x)\phi(S),\end{aligned}$$

显然, σ 是 $G \rightarrow \bar{G}/\phi(S)$ 的一个群同态.

由于 ϕ 是满的, 易知 σ 是满同态;

$$\text{Ker}\sigma = S;$$

事实上: 任意的 $x \in S$, $\phi(x) \in \phi(S)$. $\sigma(x) = [\phi(x)] = \phi(x)\phi(S) = \phi(S)$, 所以 $x \in \text{Ker}\sigma$, $S \subseteq \text{Ker}\sigma$;

任意的 $x \in \text{Ker}\sigma$, 则 $\sigma x = \phi(x)\phi(S) = \phi(S)$, 所以 $\phi(x) \in \phi(S)$, 从而存在 $s \in S$, 使得 $\phi(x) = \phi(s)$, $\phi(xs^{-1}) = e \in \bar{G}$. $xs^{-1} \in \text{Ker}\phi = H \subseteq S$, 所以存在 $h \in H$, 使得 $xs^{-1} = h$, $x = hs \in S$, 所以 $\text{Ker}\sigma \subseteq S$.

利用群的第一同态定理, 知: $G/S \cong \bar{G}/\phi(S)$. □

书后练习6.3. $P_{42}, Ex3$

证明: 1) 因为 S 是 G 的一个子群, 所以 $\phi(S)$ 是 H 的子群. 而对任意的 $s \in S$, $\phi'(s) = \phi(s) \in \phi(S)$, 且 ϕ 是群同态, 所以 ϕ' 保持运算, 从而

$$\phi' : S \rightarrow \phi(S)$$

是一个群同态. 且 ϕ' 是满射, 所以是群同态.

2) 任意的 $x \in S \cap \text{Ker}\phi$, 则 $\phi'(x) = \phi(x) = e \in \phi(S)$, $x \in \text{Ker}\phi'$, 所以 $S \cap \text{Ker}\phi \subseteq \text{Ker}\phi'$;

任意的 $x \in \text{Ker}\phi'$, 则 $x \in S$ 且 $\phi(x) = \phi'(x) = e$, $x \in \text{Ker}\phi$, 所以 $x \in S \cap \text{Ker}\phi$, $\text{Ker}\phi' \subseteq S \cap \text{Ker}\phi$;

所以, $\text{Ker}\phi' = S \cap \text{Ker}\phi$.

3) 我们要证明: $S/(S \cap \text{Ker}\phi) \cong \phi(S)$.

由于 ϕ' 是 S 到 $\phi(S)$ 的一个满同态, 且 $\text{Ker}\phi' = S \cap \text{Ker}\phi$, 利用群的第一同态定理, 即可以得到. \square

书后练习6.4. $P_{42}, Ex4$

证明: 1) 因为 H 是 G 的正规子群, S 是群 G 的一个子群, 所以 $SH = HS$ ($P_{22}, Ex3, (2)$ 的结论), 从而 SH 是 G 的子群.

任意的 $x \in H, y \in SH \subseteq G$, 由于 H 是 G 的正规子群, 所以 $yxy^{-1} \in H$, 从而 H 是 SH 的正规子群.

$S \cap H$ 是两个子群的交, 仍然是群, 是 S 的子群. 任意的 $x \in S \cap H, y \in S$, 则 $x \in H, yxy^{-1} \in H, yxy^{-1} \in S, yxy^{-1} \in S \cap H$.

所以 $S \cap H$ 是 S 的正规子群.

2) 由于 H 是 SH 的正规子群, 所以 SH/H 是商群. 作:

$$\begin{aligned}\sigma : S &\rightarrow SH/H, \\ x &\mapsto xH \in SH/H.\end{aligned}$$

则: σ 是 S 到 SH/H 的一个映射, 且任意的 $x, y \in S$,

$\sigma(xy) = xyH = (xH)(yH) = \sigma(x)\sigma(y)$, 即有: σ 是 S 到 SH/H 的一个群同态;

又 $xH \in SH/H$, 则 $x \in SH$, 存在 $s \in S, h \in H$, 使得 $x = sh$. 这时, $xH = (sh)H = s(hH) = sH$, 所以存在 $s \in S$, 满足 $\sigma(s) = \sigma(x) = xH$, σ

是 S 到 SH/H 的群满同态;

任意的 $x \in \text{Ker}\sigma$, 则 $x \in S$ 且 $\sigma(x) = xH = H$, $x \in H$, $x \in S \cap H$, $\text{Ker}\sigma \subseteq S \cap H$;

任意的 $x \in S \cap H$, 则 $x \in H$, $\sigma(x) = xH = H$, $x \in \text{Ker}\sigma$, 所以 $S \cap H \subseteq \text{Ker}\sigma$;

$S \cap H = \text{Ker}\sigma$, 由群的第一同态定理, 有: $S/S \cap H \cong SH/H$. \square

§7 有限群

书后练习7.1. P_{46} , Ex1

证明: 任取 $a \in G$, $a \neq e$, 则 a 的周期 m 不是 1, 且 $m \mid p$. 又因为 p 是素数, 所以 $m = p$. 从而 $\langle a \rangle$ 是 p 阶群, 所以 $\langle a \rangle = P$. \square

(习题实际上告诉了我们这个事实: 素数阶群一定是循环群.)

书后练习7.2. P_{46} , Ex2

证明: 因为 H 是群 G 的指数为 2 的子群, 所以群 G 关于 H 的所有左陪集为 H, aH , 其中 $a \notin H$.

注意到 $aH = H = Ha \Leftrightarrow a \in H$. 所以对任意的 $x \in G$,

若 $xH = H \Rightarrow x \in H \Rightarrow Hx = H \Rightarrow xH = Hx$;

若 $xH = aH \Rightarrow x \notin H \Rightarrow Hx \neq H \Rightarrow Hx = Ha \Rightarrow xH = Hx$;

所以 H 是 G 的正规子群. \square

书后练习7.3. P_{46} , Ex3

证明: 1) 任意的 $[a_1] = [a_2]$, $[b_1] = [b_2]$, 则 $p \mid (a_1 - a_2)$, $p \mid (b_1 - b_2)$, 而 $a_1b_1 - a_2b_2 = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2 = b_1(a_1 - a_2) + a_2(b_1 - b_2)$, 所以 $p \mid (a_1b_1 - a_2b_2)$.

$[a_1b_1] = [a_2b_2]$. 运算是良定的;

任意的 $[a], [b], [c] \in \mathbb{Z}_p \setminus \{[0]\}$, 有

$$([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a]([b][c]),$$

结合律成立;

$[1] \in \mathbb{Z}_p \setminus \{[0]\}$, 对任意的 $[a] \in \mathbb{Z}_p \setminus \{[0]\}$, 都有

$$[a][1] = [1][a] = [a],$$

$\mathbb{Z}_p \setminus \{[0]\}$ 关于乘法有单位元;

任意的 $[b] \in \mathbb{Z}_p \setminus \{[0]\}$, 则 $b \neq kp$, 从而 $(b, p) = 1$, 所以存在 $l, m \in \mathbb{Z}$, 使得

$$lb + mp = 1,$$

$$[lb + mp] = [1], [l][b] + [m][p] = [1], [l][b] = [1],$$

$[l]$ 是 $[b]$ 的逆元;

综上: $\mathbb{Z}_p \setminus \{[0]\}$ 按所定义的乘法成一个群. 它有 $p-1$ 个元素, 是 $p-1$ 阶群.

事实上: $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ 还是一个交换群.

2) 对任意整数 $a \in \mathbb{Z}$.

若 $a = kp$, 则 $p \mid (a^p - a)$, $a^p \equiv a \pmod{p}$;

若 $a \neq kp$, 则 $[a] \in \mathbb{Z}_p \setminus \{[0]\}$, 注意到 $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ 是一个 $p-1$ 阶群, 所以 $[a]^{p-1} = [1]$, 亦即 $[a^{p-1}] = [1]$, 所以 $[a^{p-1}][a] = [a]$, $[a^p] = [a]$,

$p \mid (a^p - a)$, $a^p \equiv a \pmod{p}$. □

书后练习7.4. $P_{46}, Ex4$

证明: 任意的 $g, h \in G$,

$$gSg^{-1} = hSh^{-1} \Leftrightarrow h^{-1}gSg^{-1}h = S = (h^{-1}g)S(h^{-1}g)^{-1} \Leftrightarrow h^{-1}g \in N(S)$$

$\Leftrightarrow gN(S) = hN(S)$, 亦即: $gSg^{-1} = hSh^{-1} \Leftrightarrow g, h$ 关于 G 的子群 $N(S)$ 有相同的左陪集.

所以 G 中所有与 S 共轭的子集 $\{gSg^{-1} | g \in G\}$ 的个数恰好是 G 中关于子群 $N(S)$ 的左陪集的个数. 所以

$$|O(S)| = [G : N(S)].$$

□

§8 有限交换群的结构定理

书后练习8.1. $P_{52}, Ex1$

证明: 1) 任意的 $h_i \in H_i$, $h_j \in H_j$, 由于 H_i, H_j 是 G 的子群, 所以 $h_i^{-1} \in H_i$, $h_j^{-1} \in H_j$, 利用性质 2), 则有

$$(h_i h_j)(h_i^{-1} h_j^{-1}) = (h_i h_i^{-1})(h_j h_j^{-1}) = e,$$

所以

$$(h_i^{-1} h_j^{-1})^{-1} = h_i h_j,$$

而

$$(h_i^{-1} h_j^{-1})^{-1} = (h_j^{-1})^{-1}(h_i^{-1})^{-1} = h_j h_i,$$

所以: $h_i h_j = h_j h_i$;

2) H_i 是 G 的子群, 任意的 $g \in G$, 由 1), 存在 $g_j \in H_j$, $j = 1, 2, \dots, n$, 使得

$$g = g_1 \cdots g_{i-1} g_i g_{i+1} \cdots g_n,$$

利用结论 1), 有

$$g = g_1 \cdots g_{i-1} g_{i+1} \cdots g_n g_i,$$

而任意的 $h_i \in H_i$, 利用结论 1), 有

$$(g_1 \cdots g_{i-1} g_{i+1} \cdots g_n) h_i = h_i (g_1 \cdots g_{i-1} g_{i+1} \cdots g_n) h_i,$$

且

$$h_i H_i = H_i h_i = H_i,$$

$$\begin{aligned} g H_i &= (g_1 \cdots g_{i-1} g_{i+1} \cdots g_n g_i) H_i = (g_1 \cdots g_{i-1} g_{i+1} \cdots g_n) H_i \\ &= H_i (g_1 \cdots g_{i-1} g_{i+1} \cdots g_n) = H_i (g_i g_1 \cdots g_{i-1} g_{i+1} \cdots g_n) \\ &= H_i (g_1 \cdots g_{i-1} g_{i+1} \cdots g_n g_i) = H_i g, \end{aligned}$$

所以 H_i 是 G 的正规子群.

3) G 是 $H_{i_1}, H_{i_2}, \dots, H_{i_n}$ 的内直积, 就要说明:

(3.1) $G = H_{i_1} H_{i_2} \cdots H_{i_n}$. 这是因为: 由结论 1), 任意的 i, j , 都有 $H_i H_j = H_j H_i$. 所以

$$G = H_1 H_2 \cdots H_n = H_{i_1} H_{i_2} \cdots H_{i_n}.$$

(3.2) 任意的 $h_{i_j}, h'_{i_j} \in H_{i_j}$, $j = 1, 2, \dots, n$, 由结论 1),
 $(h_{i_1} h_{i_2} \cdots h_{i_n})(h'_{i_1} h'_{i_2} \cdots h'_{i_n}) = (h_1 h_2 \cdots h_n)(h'_1 h'_2 \cdots h'_n)$
 $= (h_1 h'_1)(h_2 h'_2) \cdots (h_n h'_n) = (h_{i_1} h'_{i_1})(h_{i_2} h'_{i_2}) \cdots (h_{i_n} h'_{i_n});$

(3.3) 假设 $g = g_{i_1}g_{i_2}\cdots g_{i_n} = g'_{i_1}g'_{i_2}\cdots g'_{i_n}$, 其中 $g_{i_j}, g'_{i_j} \in H_{i_j}$, $j = 1, 2, \dots, n$. 则利用结论 1), 有:

$$\begin{aligned} g &= g_{i_1}g_{i_2}\cdots g_{i_n} = g'_{i_1}g'_{i_2}\cdots g'_{i_n} \\ &= g_1g_2\cdots g_n = g'_1g'_2\cdots g'_n, \quad g_j, g'_j \in H_j, \quad j = 1, 2, \dots, n, \end{aligned}$$

由条件 c), 则 $g_j = g'_j, j = 1, 2, \dots, n$. 所以 $g_{i_j} = g'_{i_j}, j = 1, 2, \dots, n$.

所以, G 是 $H_{i_1}, H_{i_2}, \dots, H_{i_n}$ 的内直积.

4) 由 c) 知道 g_i 被 g 唯一确定, 所以 ϕ_i 是 G 到 H_i 的一个映射. 且

$$(4.1) \text{ 对任意的 } g_i \in H_i, \text{ 存在 } g = \underbrace{e \cdots e}_{i-1} g_i \underbrace{e \cdots e}_{n-i} \in G, \text{ 使得 } \phi_i(g) = g_i,$$

亦即 ϕ_i 是满射;

(4.2) 对任意的 $g, h \in G, g = g_1g_2\cdots g_n, h = h_1h_2\cdots h_n, g_j, h_j \in H_j$, 则由 b) 得到: $gh = (g_1h_1)(g_2h_2)\cdots(g_nh_n)$, 从而

$$\phi_i(gh) = g_ih_i = \phi_i(g)\phi_i(h),$$

所以 ϕ_i 保持群的运算;

所以, ϕ_i 是群 G 到 H_i 的一个群同态.

(4.3) 任取 $g = g_1\cdots g_{i-1}g_{i+1}\cdots g_n \in H_1\cdots H_{i-1}H_{i+1}\cdots H_n$, 则 $g = g_1\cdots g_{i-1}eg_{i+1}\cdots g_n \in H_1\cdots H_{i-1}H_iH_{i+1}\cdots H_n$, $\phi_i(g) = e, g \in \text{Ker}\phi_i$;

任取 $g \in \text{Ker}\phi_i$, 可设 $g = g_1\cdots g_{i-1}g_i g_{i+1}\cdots g_n$, 则 $\phi_i(g) = g_i = e$, 所以 $g = g_1\cdots g_{i-1}eg_{i+1}\cdots g_n = g_1\cdots g_{i-1}g_{i+1}\cdots g_n \in H_1\cdots H_{i-1}H_{i+1}\cdots H_n$;

所以 $\text{Ker}\phi_i = H_1\cdots H_{i-1}H_{i+1}\cdots H_n$. \square

书后练习8.2. $P_{53}, Ex2$

证明: 由于 $h_1h_2\cdots h_n$ 完全被 (h_1, h_2, \dots, h_n) 确定, 所以 ϕ 是 \bar{G} 到 G 的一个映射, 且

$$\begin{aligned} (1) \text{ 任取 } \bar{g}, \bar{h} \in \bar{G}, \bar{g} &= (g_1, g_2, \dots, g_n), \bar{h} = (h_1, h_2, \dots, h_n), \text{ 则:} \\ \bar{g}\bar{h} &= (g_1h_1, g_2h_2, \dots, g_nh_n), \\ \phi(\bar{g}\bar{h}) &= (g_1h_1)(g_2h_2)\cdots(g_nh_n) = (g_1g_2\cdots g_n)(h_1h_2\cdots h_n) = \phi(\bar{g})\phi(\bar{h}); \end{aligned}$$

所以 ϕ 是 \bar{G} 到 G 的一个群同态;

(2) 任取 $g \in G$, 则存在 $g_i \in H_i, i = 1, 2, \dots, n$, 使得 $g = g_1g_2\cdots g_n$, 从而存在 $\bar{g} = (g_1, g_2, \dots, g_n) \in \bar{G}$, 满足 $\phi(\bar{g}) = g$.

所以 ϕ 是 \bar{G} 到 G 的一个满群同态;

(3) 任取 $\bar{g}, \bar{h} \in \bar{G}$, $\bar{g} = (g_1, g_2, \dots, g_n)$, $\bar{h} = (h_1, h_2, \dots, h_n)$, 则:
 $\phi(\bar{g}) = g_1 g_2 \cdots g_n$, $\phi(\bar{h}) = h_1 h_2 \cdots h_n$,

若 $\phi(\bar{g}) = \phi(\bar{h})$, 则 $g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_n \in G$, 注意到 G 是 H_i 的内直积; 由 c), 则 $g_i = h_i$ $i = 1, 2, \dots, n$, 从而:

$$(g_1, g_2, \dots, g_n) = (h_1, h_2, \dots, h_n).$$

所以 ϕ 是 \bar{G} 到 G 的一个单群同态;

所以 ϕ 是 \bar{G} 到 G 的一个群同构. □

书后练习8.3. P_{53} , Ex3

证明: 由于 $G = H_1 H_2$ 是内直积, 所以存在 G 在分量 H_1 投影

$$\begin{aligned}\phi_1 : G &\rightarrow H_1, \\ g &\mapsto h_1,\end{aligned}$$

则 ϕ_1 是 G 到 H_1 的满同态, 且 $\text{Ker} \phi_1 = H_2$, 利用群的第一同态定理, 则

$$H_1 \cong G/H_2;$$

同样可以证明:

$$H'_1 \cong G/H_2;$$

再由群同构的传递性, $H_1 \cong H'_1$.

例如, Klein 四元群. $K = \{e, a, b, ab\}$, 其中 e 是单位元, $a^2 = b^2 = (ab)^2 = e$.

记 $H_1 = \langle a \rangle$, $H'_1 = \langle b \rangle$, $H_2 = \langle ab \rangle$, 则 $K = H_1 H_2 = H'_1 H_2$ 是内直积, $H_1 \cong H'_1$, 但 $H_1 \neq H'_1$. □

书后练习8.4. P_{53} , Ex4

证明: 我们对 n 进行归纳.

$n = 1$ 时, 结论是平凡的;

$n = 2$ 时, 设 $G = \langle a_1 \rangle \langle a_2 \rangle$ 是内直积, 且 a_i 的周期是 m_i , $i = 1, 2$, 且 $(m_1, m_2) = 1$.

因为 G 是 $\langle a_1 \rangle$ 与 $\langle a_2 \rangle$ 的内直积, 且 $\langle a_1 \rangle$, $\langle a_2 \rangle$ 都是有限阶群, 所以 $|G| \leq |\langle a_1 \rangle| \cdot |\langle a_2 \rangle| = m_1 m_2$.

又因为 $a_1 a_2 \in G$, 且 $(a_1 a_2)^{m_1 m_2} = (a_1)^{m_1 m_2} (a_2)^{m_1 m_2} = e$, 所以 $(a_1 a_2)$ 的阶数是 $m_1 m_2$ 的因数. 设 $(a_1 a_2)$ 的阶数为 l , 则 $l \mid m_1 m_2$, 且 $(a_1 a_2)^l = (a_1)^l (a_2)^l = e$, 而 $e = e \cdot e$ 且 $G = \langle a_1 \rangle \langle a_2 \rangle$ 是内直积, 所以 $(a_1)^l (a_2)^l = e$ 必须 $(a_1)^l = (a_2)^l = e$, 从而 $m_1 \mid l, m_2 \mid l$, l 是 m_1, m_2 的公倍数, 注意 l 有最小性, 所以 $l = [m_1, m_2]$ 是 m_1, m_2 的最小公倍数.

又因为 m_1, m_2 互素, 所以 $l = [m_1, m_2] = m_1 m_2$ 是 $a_1 a_2$ 的阶, G 是 $m_1 m_2$ 阶循环群.

假设 $n = k$ 时结论成立. 当 $n = k + 1$ 时, 记 $H = \langle a_1 \rangle \cdots \langle a_k \rangle$, 则 H 是 $\langle a_1 \rangle, \dots, \langle a_k \rangle$ 的内直积, 且满足归纳假设的条件, 从而 H 是阶数为 $m_1 \cdots m_k$ 的循环群, 其生成元为 $a_1 \cdots a_k$, 亦即 $H = \langle a_1 \cdots a_k \rangle$.

显然, $G = H \cdot \langle a_{k+1} \rangle$ 是直积, H 是 $m_1 \cdots m_k$ 阶循环群, $\langle a_{k+1} \rangle$ 是 m_{k+1} 阶循环群, 且 $(m_1 \cdots m_k, m_{k+1}) = 1$, 利用前面的结论, 则有: $G = \langle (a_1 \cdots a_k) \cdot a_{k+1} \rangle$ 是 $(m_1 \cdots m_k \cdot m_{k+1})$ 阶循环群. \square

§9 单群

书后练习9.1. $P_{58}, Ex1$

证明:任取 S_n 的一个 2 阶子群 $H = \{e, \sigma\}$, 其中 $\sigma^2 = e$, e 为恒等置换.

假若 H 是 S_n 的正规子群, 则对任意的 $\alpha \in S_n$, 都有 $\alpha \sigma \alpha^{-1} \in H$.

由于任何一个置换都可以表成若干不相交轮换的积, 所以可设

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_s,$$

其中, $\gamma_1, \gamma_2, \dots, \gamma_s$ 是不相交的非恒等置换.

假若 γ_i 的阶数为 t_i , 注意到不相交置换是可交换的, 因而 $\gamma_1 \gamma_2 \cdots \gamma_s$ 的阶为 $[t_1, \dots, t_s]$ 为 t_1, \dots, t_s 的最小公倍数. 注意到 $\sigma^2 = e$, 所以 $t_1 = \cdots = t_s = 2$.

可设 $\sigma = (i_1 i_2)(i_3 i_4) \cdots (i_{j-1} i_j)$, 因为 $n \geq 3$, 所以至少存在一个 3-轮换 $(i_1 i_2 i_3)$, 取 $\alpha = (i_1 i_2 i_3)$, 则 $\alpha^{-1} = (i_3 i_2 i_1)$. 这时

$$\begin{aligned} \alpha \sigma \alpha^{-1} &= (i_1 i_2 i_3)(i_1 i_2)(i_3 i_4) \cdots (i_{j-1} i_j)(i_3 i_2 i_1) \\ &= (i_1 i_2 i_3)(i_1 i_2)(i_3 i_4)(i_3 i_2 i_1) \cdots (i_{j-1} i_j) \end{aligned}$$

$$= (i_1 i_3)(i_2 i_4) \cdots (i_{j-1} i_j) \in H$$

所以 H 不是 S_n 的正规子群. □

书后练习9.2. $P_{58}, Ex2$

证明: $S_n, A_n, \{(1)\}$ 是 S_n 的当然正规子群.

$n = 1, 2$ 时, 结论显然;

$n = 3$ 时, $|S_3| = 6$, 它有 2, 3 阶非平凡子群. 而其 3 阶子群为 A_3 , 是其正规子群;

下说明: 其 2 阶子群不是正规子群. S_3 的 2 阶子群只能是 $H = \{(1), (i_1 i_2)\}$. 由于存在 $(i_1 i_2 i_3) \in S_3$, 且

$$(i_1 i_2 i_3)(i_1 i_2)(i_1 i_2 i_3)^{-1} = (i_1 i_3) \notin H,$$

所以 H 不是 S_3 的正规子群;

$n \geq 5$ 时, 注意 A_5 是单群, 若 H 是 S_n 的异于 $S_n, A_n, \{(1)\}$ 正规子群, 则 H 不是 A_n 的正规子群, 也就是说 H 不是 A_n 的子群. (若 H 是 A_n 的子群, 必是 A_n 的正规子群.)

考虑: $K = H \cap A_n$, 则任意 $\alpha \in S_n, \beta \in K$, 则

$$\beta \in H, \alpha\beta\alpha^{-1} \in H,$$

$$\beta \in A_n, \alpha\beta\alpha^{-1} \in A_n$$

从而 $\alpha\beta\alpha^{-1} \in K$, K 是 S_n 的正规子群.

注意到 K 也是 A_n 的正规子群, 所以 $K = \{(1)\}$ 或 $K = A_n$.

若 $K = A_n$, 由于 K 是 H 的子群, 所以 A_n 是 H 的子群, 注意到 A_n 的指数为 2, 所以不存在 H , 满足

$$A_n \subsetneq H \subsetneq S_n,$$

($|A_n|$ 是 $|S_n|$ 的最大真因数). 矛盾.

所以 $K = \{(1)\}$.

若 $K = \{(1)\}$, 则 H 中除单位以外没有其他偶置换. 因为任何两个奇置换之积为偶置换, 所以任意 $\alpha, \beta \in H$, 必有 $\alpha\alpha = \alpha\beta = (1)$, 从而 H 是一个 2 阶子群. 再由 $Ex1$, 矛盾.

所以 S_n 没有异于 $S_n, A_n, \{(1)\}$ 的正规子群. □

§10 群的构造, 自由群

§11 群在集上的作用

书后练习11.1. $P_{71}, Ex1$

证明: (1) 任意的 $g \in G, H \in M$, 要验证 $gHg^{-1} \in M$ (仍是 G 的子群), 事实上:

$$(gHg^{-1})(gHg^{-1}) = gHHg^{-1} = gHg^{-1}, (gHg^{-1})^{-1} = (g^{-1})^{-1}H^{-1}g^{-1}.$$

对任意的 $H \in M$ 以及 $e \in G$, 有 $e \times H = eHe^{-1} = H$;

对任意的 $g, h \in G, H \in M$, 有 $g \times (h \times H) = g \times (hHh^{-1}) = g(hHh^{-1})g^{-1} = (gh)H(gh)^{-1} = (gh) \times H$.

(2) H 是 G 的正规子群

$$\Leftrightarrow \text{任意 } g \in G, \text{ 都有 } gHg^{-1} = H$$

$$\Leftrightarrow \text{任意 } g \in G, \text{ 都有 } g \in S_H$$

$$\Leftrightarrow S_H = G$$

□

书后练习11.2. $P_{71}, Ex2$

证明: (1) 首先要说明: 任意 $g \in G$, 都有 $gA \in M$, 亦即 gA 也是 G 中含 m 个元素的子集. 事实上: 定义映射

$$\phi: A \rightarrow gA$$

$$a \mapsto ga,$$

则:

任意 $a_1, a_2 \in A$, 若 $ga_1 = ga_2$, 由群中运算的消去律, $a_1 = a_2$, ϕ 是单射;

任意 $x \in gA$, 存在 $a \in A$ 使得 $x = ga$, 从而 $\phi(a) = ga = x$, ϕ 是满射.

再: 任意 $A \in M$, e 是 G 的单位元, 容易知道: $e \times A = eA = A$;

任意 $A \in M, g, h \in G$, 有

$$g \times (h \times A) = g \times (hA) = g(hA) = (gh)A = (gh) \times A.$$

(2) 因为 $\forall s \in S_A, a \in A$, 有 $s \times a = sa \in A$, 所以集 A 可以看作一个 S_A -集.

在 A 上定义一个关系 $\sim: x \sim y \Leftrightarrow$ 存在 $s \in S_A$, 使得 $sx = y$. 则 \sim 是 A 上的一个等价关系. x 在 S_A -集 A 中的轨道 O_x 是元素 x 在等价关系 \sim 下的等价类. 且 $A = \bigcup_{x \in A} O_x$.

下证: 对任意的 $x \in A$, 都 $|S_A| = |O_x|$. 事实上, 作 S_A 到 O_x 的一个映射:

$$\begin{aligned}\phi: S_A &\rightarrow O_x \\ s &\mapsto sx,\end{aligned}$$

因为任意的 $s_1, s_2 \in S_A$, 有 $s_1x = s_2x \Rightarrow s_1 = s_2$, ϕ 是单射;

又任意 $y \in O_x$, 存在 $s \in S_A$, 使得 $y = sx$, 从而存在 $s \in S_A$, 满足 $\phi(s) = sx = y$, ϕ 是满射.

所以任意的 $x, y \in A$, $|S_A| = |O_x| = |O_y|$, 又 A 是有限集, 它是有限个不相交的 O_x 的并集, 所以 $|A|$ 是 $|O_x|$ 的倍数.

所以 $|S_A| \mid m$. □

§12 本章总习题

书后练习12.1. $P_{71}, Ex1$

证明: (1) 由 $a^{[s,t]} = (a^s)^{\frac{[s,t]}{s}} \in \langle a^s \rangle \Rightarrow \langle a^{[s,t]} \rangle \subseteq \langle a^s \rangle$;
同理, $\langle a^{[s,t]} \rangle \subseteq \langle a^t \rangle$; 所以 $\langle a^{[s,t]} \rangle \subseteq \langle a^s \rangle \cap \langle a^t \rangle$;

任取 $x \in \langle a^s \rangle \cap \langle a^t \rangle$, 则 $x \in \langle a^s \rangle$, 存在整数 k , 使得 $x = a^{ks}$; $x \in \langle a^t \rangle$, 存在整数 l , 使得 $x = a^{lt}$; 所以 $x = a^m$ 且 $s \mid m, t \mid m$.
亦即: 存在整数 n , 使得 $x = a^{[s,t]n} = (a^{[s,t]})^n \in \langle a^{[s,t]} \rangle$; 所以 $\langle a^s \rangle \cap \langle a^t \rangle \subseteq \langle a^{[s,t]} \rangle$;

所以 $\langle a^s \rangle \cap \langle a^t \rangle = \langle a^{[s,t]} \rangle$.

(2) 由 $a^s \in a^{(s,t)}, a^t \in a^{(s,t)}$, 则
 $\langle a^s \rangle \subseteq \langle a^{(s,t)} \rangle, \langle a^t \rangle \subseteq \langle a^{(s,t)} \rangle$, 所以 $\langle a^s \rangle \cdot \langle a^t \rangle \subseteq \langle a^{(s,t)} \rangle$;

任意 $x \in \langle a^{(s,t)} \rangle$, 则存在整数 l , 使得 $x = a^{(s,t)l}$. 由于存在整数 m, n , 满足 $ms + nt = (s, t)$, 所以

$$x = a^{(s,t)l} = (a^{(s,t)})^l = (a^{(ms+nt)})^l = (a^s)^{ml} \cdot (a^t)^{nl} \in \langle a^s \rangle \cdot \langle a^t \rangle,$$

所以 $\langle a^{(s,t)} \rangle \subseteq \langle a^s \rangle \cdot \langle a^t \rangle$;

所以 $\langle a^s \rangle \cdot \langle a^t \rangle = \langle a^{(s,t)} \rangle$. □

书后练习12.2. P_{71} , Ex2

证明: 由 G 中元素的阶均不大于 2, 所以任意 $a \in G$, 都有 $a^2 = e$, e 为 G 的单位元. 所以对任意 $a \in G$, $a^{-1} = a$.

任意 $a, b \in G$, $(ab)^{-1} = ab$, 且 $(ab)^{-1} = b^{-1}a^{-1} = ba$, 所以 $ab = ba$, G 是交换群. □

书后练习12.3. P_{71} , Ex3

证明: 由 $H \subseteq C(G)$, 所以 H 是 G 的正规子群, G/H 是商群.

G/H 是循环群, 可设 $G/H = \langle \bar{a} \rangle$, $a \in G$. 任意 $x, y \in G$, 考虑 x, y 所在的陪集 \bar{x}, \bar{y} , 则存在整数 k, l , 使得 $\bar{x} = (\bar{a})^k$, $\bar{y} = (\bar{a})^l$. 从而存在 $c_1, c_2 \in C(G)$, 满足 $x = a^k c_1$, $y = a^l c_2$.

所以 $xy = a^k c_1 a^l c_2 = a^k a^l c_1 c_2 = a^l a^k c_1 c_2 = a^l c_2 a^k c_1 = yx$, 亦即: G 是一个交换群. □

书后练习12.4. P_{72} , Ex4

证明: 设群 G 的阶为 p^2 , 则 G 中元素的阶为 1, p , p^2 .

若 G 中存在 p^2 阶元素, 则 G 是一个循环群, 是交换群;

若 G 中没有 p^2 阶元素, 则 G 中除去单位元以外, 都是 p 阶元素. 任取 $a, b \in G$. 则 $a^p = b^p = e$, 且任意 $0 < s < p$, 都有 $a^s \neq e$, $b^s \neq e$, e 为 G 的单位元. 且 $(ab)^p = e \Rightarrow (ab)^p = e = a^p b^p \Rightarrow (ab)^{p-1} = a^{p-1} b^{p-1}$.

注意到: $(ab)^{-1} = (ab)^{p-1}$, $(a)^{-1} = (a)^{p-1}$, $(b)^{-1} = (b)^{p-1}$,

所以 $(ab)^{-1} = a^{-1} b^{-1} \Rightarrow b^{-1} a^{-1} = a^{-1} b^{-1} \Rightarrow (b^{-1} a^{-1})^{-1} = (a^{-1} b^{-1})^{-1} \Rightarrow ab = ba$.

所以 G 是交换群. □

书后练习12.5. P_{72} , Ex5

证明: 因为 G 是一个交换群, 且 $|G| = p_1 p_2 \cdots p_t$, $p_i, i = 1, 2, \dots, t$ 是互不相同的素数, 利用引理 7.6(见教材 P_{33}), G 中存在 p_i 阶元, $i = 1, 2, \dots, t$.

记 G 的 p_i 阶元为 $a_i, i = 1, 2, \dots, t$. 考虑 $H = \langle a_k \rangle \cdot \langle a_l \rangle$, 由于 G 是交换群, 所以 $H = \langle a_k \rangle \cdot \langle a_l \rangle$ 是 G 的子群, 且 $\langle a_k \rangle, \langle a_l \rangle$ 是 H

的子群; 从而 $p_k \mid |H|$, $p_l \mid |H|$, $|H|$ 是子群 H 的阶. 由于 p_k, p_l 是不同的素数, $(p_k, p_l) = 1$, 所以 H 是 $p_k p_l$ 阶群.

考虑 $a_k a_l$ 的阶数. 显然, $a_k a_l$ 的阶是 $p_k p_l$ 的因数, 注意到: p_k, p_l 是不同的素数, 所以 $a_k a_l$ 的阶只能是: $1, p_k, p_l, p_k p_l$.

若 $a_k a_l$ 的阶为 1 , 则 $a_k a_l = e$, 从而 $a_k^{-1} = a_l$, 它们有相同的阶;

若 $a_k a_l$ 的阶为 p_k , 则 $(a_k a_l)^{p_k} = a_k^{p_k} a_l^{p_k} = a_l^{p_k} = e$, 矛盾;

若 $a_k a_l$ 的阶为 p_l , 则 $(a_k a_l)^{p_l} = a_k^{p_l} a_l^{p_l} = a_k^{p_l} = e$, 矛盾;

所以, $a_k a_l$ 的阶为 $p_k p_l$, 所以 $H = \langle a_k a_l \rangle$ 是循环群;

下面证明: $a_1 a_2 \cdots a_t$ 的阶数为: $p_1 p_2 \cdots p_t$. 记 $H = \langle a_1 \rangle \cdot \langle a_2 \rangle \cdots \langle a_t \rangle$, 则 H 是 G 的一个子群, 且 $\langle a_k \rangle$ 是 H 的子群, 所以 $p_k \mid |H|$, $|H|$ 是 H 的阶. 注意到 $p_i, i = 1, 2, \dots, t$ 是互不相同的素数, 所以 $|H| = p_1 p_2 \cdots p_t$;

利用已知定理, $a_1 a_2 \cdots a_t$ 的阶数为 $p_1 p_2 \cdots p_t$ 的因数,

记为 $s = p_{i_1} \cdots p_{i_m}, 1 \leq i_1 \leq \dots \leq i_m \leq t$,

这时 $(a_{i_l})^s = e$, 所以 $(a_1 a_2 \cdots a_t)^s = (a_{j_1} \cdots a_{j_{t-m}})^s = e$.

考虑 $K = \langle a_{j_1} \rangle \cdots \langle a_{j_{t-m}} \rangle$, 则 K 是 G 的子群, 且 K 的阶数为 $l = p_{j_1} \cdots p_{j_{t-m}}$; 但 $(a_{j_1} \cdots a_{j_{t-m}})$ 是 K 中的 s 阶元, 所以 $s \mid l$, 矛盾.

所以 $a_1 a_2 \cdots a_t$ 的阶数为: $p_1 p_2 \cdots p_t$.

亦即: G 是循环群, $a_1 a_2 \cdots a_t$ 是它的生成元. □

书后练习12.6. $P_{72}, Ex6$

证明: □

书后练习12.7. $P_{72}, Ex7$

证明: A, B 是群 G 的两个有限子群, 所以 $A \cap B$ 是群. 任意 $h \in H, x \in AB$, 定义:

$$h \times x = hx,$$

则: \times 是群 H 在集 AB 上的作用.

在 AB 上定义关系: $x \sim y \Leftrightarrow$ 存在 $h \in H$, 使得 $h \times x = y$. 则 \sim 是 AB 上的等价关系.

任意 $x \in AB$, 记 $O_x = \{hx \mid \forall h \in H\}$ 为 x 所在的轨道, 是 x 在等价关系 \sim 下的等价类, 则: $AB = \bigcup_{x \in AB} O_x$.

如下首先证明: 任意 $x \in AB$, 都有 $|O_x| = |A \cap B|$.

事实上: 作 H 到 O_x 的一个对应:

$$\begin{aligned}\phi: H &\rightarrow O_x, \\ h &\mapsto hx.\end{aligned}$$

则: (1) $h_1x = h_2x \Rightarrow h_1 = h_2$, ϕ 是单射;

(2) 任意 $y \in O_x$, 则存在 $h \in H$, 使得 $hx = y$, ϕ 是满的.

所以 $|AB|$ 等于不相交轨道个数乘 $|A \cap B|$.

再证明: AB 的不相交轨道个数等于 A 中不相交轨道个数与 B 中不相交轨道个数之积.

首先, 由于 A 是群, 所以任意 $x \in A$, $h \in H \subset A$, 都有 $hx \in A$, 所以 O_x 是 A 的子集, 同样, 任意 $y \in B$, 有 O_y 是 B 的子集.

设 $a_i \in A$, $b_i \in B$, 且 $O_{a_1} \neq O_{a_2}$, $O_{b_1} \neq O_{b_2}$, 则任意 $h \in H$, $ha_1 \neq a_2$, $hb_1 \neq b_2$, 亦即 $a_2a_1^{-1} \notin H$, $b_2b_1^{-1} \notin H$.

若 $O_{a_1b_1} = O_{a_2b_2}$, 则存在 $h \in H$, 使得:

$$ha_1b_1 = a_2b_2 \Rightarrow a_2^{-1}ha_1 = b_2b_1^{-1} \Rightarrow b_2b_1^{-1} \in H \Rightarrow \text{矛盾}.$$

所以, AB 中不相交轨道的个数等于 A 中不相交轨道的个数与 B 中不相交轨道的个数之积.

$$\text{亦即: } \frac{|AB|}{|A \cap B|} = \frac{|A|}{|A \cap B|} \frac{|B|}{|A \cap B|}, \text{ 所以 } |AB| = \frac{|A||B|}{|A \cap B|}. \quad \square$$

书后练习12.8. $P_{72}, Ex8$

证明: 由 $H \subseteq K \subseteq G$ 且 $[G:H]$ 是有限数, 所以 $[G:K] \leq [G:H]$, $[K:H] \leq [G:H]$ 都是有限数.

记 $[G:K] = s$, $[K:H] = t$, 且 k_1H, k_2H, \dots, k_tH 是商集 K/H 中的 t 个元素, $k_lH = k_mH \Leftrightarrow k_l = k_m$; g_1K, g_2K, \dots, g_sK 是商集 G/K 中的 s 个元素, $g_lK = g_mK \Leftrightarrow g_l = g_m$. 如下要证明: g_ik_jH 是商集 G/H 中不同的元素, $i = 1, 2, \dots, s$, $j = 1, 2, \dots, t$.

任意的 $x \in G$, 则存在 $g_i \in G$, 使得 $g_iK = xK$, 所以 $g_i^{-1}x \in K$, 从而存在 $k_j \in K$, 使得 $g_i^{-1}xH = k_jH$, 亦即: $xH = g_ik_jH$, 所以 $G/H \subseteq \{g_ik_jH | i = 1, 2, \dots, s; j = 1, 2, \dots, t\}$;

再: 任意 $g_i k_j H = g_l k_m H$, 则 $(g_l k_m)^{-1}(g_i k_j) \in H \subseteq K$, 所以
 $k_m^{-1} g_l^{-1} g_i k_j \in K \Rightarrow g_l^{-1} g_i \in K \Rightarrow g_l K = g_i K \Rightarrow g_l = g_i$
 $\Rightarrow k_j H = k_m H \Rightarrow k_j = k_m$;

所以商集 G/H 中的元素个数为 st 个.

从而 $[G : H] = [G : K][K : H]$. □

书后练习12.9. $P_{72}, Ex9$

证明: 利用 $Ex7, 8$ 的结论:

$[G : A \cap B] = [G : A][A : A \cap B]$, $[G : A \cap B] = [G : B][B : A \cap B]$, 且集合 $\{x(A \cap B) \mid x \in A\}$ 与集合 $\{yB \mid y \in AB\}$ 之间存在一个一一对应.

事实上: 作 $\{x(A \cap B) \mid x \in A\}$ 到 $\{yB \mid y \in AB\}$ 的对应:

$$\begin{aligned}\phi: \{x(A \cap B) \mid x \in A\} &\rightarrow \{yB \mid y \in AB\}, \\ x(A \cap B) &\mapsto xB,\end{aligned}$$

则: (1) $x_1(A \cap B) = x_2(A \cap B) \Rightarrow x_2^{-1}x_1 \in A \cap B \subseteq B$

$\Rightarrow x_1 B = x_2 B \Rightarrow \phi$ 是映射;

(2) $y_1 B = y_2 B, y_i \in A, i = 1, 2 \Rightarrow y_2^{-1}y_1 \in B \Rightarrow y_2^{-1}y_1 \in A \cap B$
 $\Rightarrow y_1(A \cap B) = y_2(A \cap B), \phi$ 是单射;

(3) 任意 $yB \in \{yB \mid y \in AB\}$, 存在 $z \in A$, 使得 $zB = yB$, 从而 $\phi(z(A \cap B)) = zB = yB, \phi$ 是满射.

记 $\{yB \mid y \in AB\}$ 的元素个数为 t , 显然 $t \leq [G : B]$, 所以

$$[G : A \cap B] = [G : A][A : A \cap B] = [G : A]t \leq [G : A][G : B].$$

等号成立 $t = [G : B] \Leftrightarrow G = AB \Leftrightarrow AB = BA = G$.

书后练习12.10. $P_{72}, Ex10$

解: 任取 $\phi \in \text{Aut}(G)$, 则 $\phi(G) = G = \langle a \rangle$ 仍是循环群. 所以 ϕ 完全被 $\phi(a)$ 所确定.

若 $G = \langle a \rangle$ 是无限循环群, 则 G 只有两个生成元 a, a^{-1} , 所以 $\phi(a)$ 只有两种可能:

$$\phi(a) = a \text{ 或 } \phi(a) = a^{-1},$$

这时, $\text{Aut}(G) = \{I, \phi\}$, 其中 $\phi(a) = a^{-1}$.

若 $G = \langle a \rangle$ 是有限循环群. 设 $G = \langle a \rangle$ 是 n 阶循环群. 对任意 $a^k \in G$, $0 < k < n$, 则 a^k 是 G 的生成元 $\Leftrightarrow (k, n) = 1$.

当 n 是素数时, 任取 $0 < k < n$, 记 $\phi_k(a) = a^k$, 则 $\phi_k \in \text{Aut}(G)$, 所以 $\text{Aut}(G) = \{\phi_1, \phi_2, \dots, \phi_{n-1}\}$;

对一般的正整数 n , 记 $K = \{k \mid 0 < k < n-1, (n, k) = 1\}$, 对任意 $k \in K$, 记

$$\phi_k : \phi_k(a) = a^k,$$

则 $\phi_k \in \text{Aut}(G)$, 且 $\text{Aut}(G) = \{\phi_k \mid k \in K\}$.

书后练习12.11. $P_{72}, Ex11$

证明: 任意的 $T_g \in \text{Inn}(G)$, 则:

$$\begin{aligned} T_g : G &\rightarrow G \\ x &\mapsto gxg^{-1}. \end{aligned}$$

且 $T_g = T_e$ 为 $\text{Inn}(G)$ 的单位元 $\Leftrightarrow g \in C(G)$, $C(G)$ 是 G 的中心.

作 G 到 $\text{Inn}(G)$ 的映射 ϕ :

$$\begin{aligned} \phi : G &\rightarrow \text{Inn}(G) \\ g &\mapsto T_g \end{aligned}$$

则 ϕ 是群 G 到群 $\text{Inn}(G)$ 的一个满同态映射, 且 $\text{Ker}\phi = C(G)$, 由第一同态定理, 有

$$G/C(G) \cong \text{Inn}(G).$$

□

书后练习12.12. $P_{72}, Ex12$

证明: (1) 因为

$$\begin{aligned} H_{g_1a} = H_{g_2a} &\Leftrightarrow (g_1a)(g_2a)^{-1} \in H \\ &\Leftrightarrow g_1aa^{-1}g_2 \in H \Rightarrow g_1g_2 \in H \Rightarrow g_1H = g_2H, \end{aligned}$$

所以 ι_a 是 M 上的单射;

任意 $H_x \in M$, 存在 $H_{xa^{-1}} \in M$, 使得: $\iota_a(H_{xa^{-1}}) = H_{(xa^{-1})a} = H_x$, 所以 ι_a 是满射;

所以 $\iota_a \in T(M)$;

再: $H_g(\iota_a\iota_b) = (H_g\iota_a)\iota_b = (H_{ga})\iota_b = H_{gab} = (H_g)\iota_{ab}$, 所以 $\iota_a\iota_b = \iota_{ab}$.

(2) 显然, ϕ 是 G 到 $T(M)$ 的映射, 且 $\phi(ab) = \iota_{ab} = \iota_a \iota_b = \phi(a)\phi(b)$, 所以 ϕ 是群同态.

$T(M)$ 中的单位元 ι_a , 则对任意 $g \in G$, 都有 $\iota_a(H_g) = H_{ga} = H_g$, 从而 $gag^{-1} \in H$, 所以 ι_a 是单位元 \Leftrightarrow 对任意 $g \in G$, 都有 $gag^{-1} \in H$;

由 $\text{Ker}\phi = \{a \in G \mid \iota_a = \iota_e\} = \{a \in G \mid gag^{-1} \in H, \forall g \in G\}$
 $= \{a \in G \mid a \in g^{-1}Hg, \forall g \in G\} = \{a \in G \mid a \in \bigcap_{g \in G} g^{-1}Hg\} = \bigcap_{g \in G} g^{-1}Hg. \quad \square$

书后练习12.13. $P_{72}, Ex13$

证明: 记 $M = \{Hg \mid \forall g \in G\}$, 则 M 是一个元素个数为 n 的有限集.

再记 $T(M) = \{t_a \mid a \in G, \text{其中}, t_a: G \rightarrow G, H_g \mapsto H_{ga}\}$, 由 $Ex12$ 的结论知道, $T(M)$ 是 M 上置换群 S_M 的子群.

作 G 到 $T(M)$ 的群同态 ϕ

$$\begin{aligned} \phi: G &\rightarrow T(M) \\ a &\mapsto t_a, \end{aligned}$$

则 ϕ 是满群同态, 记 $K = \text{Ker}\phi$, 则 K 是 G 的正规子群, 且 $G/K \cong T(M)$, 所以 $[G:K] = |T(M)|$.

注意 $T(M)$ 是 S_M 的子群, 所以 $|T(M)| \mid n!$, 从而 $[G:K] \mid n!$, 命题成立. \square

书后练习12.14. $P_{72}, Ex14$

证明:

\square

书后练习12.15. $P_{72}, Ex15$

证明:

\square

第三章：环、域与模

§1 环与域

书后练习1.1. $P_{83}, Ex1$

证明： (1) $0 \in C(R)$, $C(R) \neq \emptyset$;

任意 $x, y \in C(R)$, $z \in R \Rightarrow xz = zx, yz = zy$
 $\Rightarrow (x \pm y)z = xz \pm yz = zx \pm zy = z(x \pm y) \Rightarrow x \pm y \in C(R)$;
 $(xy)z = x(yz) = x(zx) = (xz)y = (zx)y = z(xy) \Rightarrow xy \in C(R)$;

所以 $C(R)$ 是 R 的子环;

(2) R 是除环 \Rightarrow 任意 $s \in R$, 存在 $t \in R$, 满足 $st = ts = 1$, 1 为 R 的单位元.

$C(R)$ 显然是交换环; 只要证: 任意 $x \in C(R)$, 都有 $x^{-1} \in C(R)$.

事实上: 任意 $x \in C(R)$, $z \in R \Rightarrow xz^{-1} = z^{-1}x \Rightarrow (xz^{-1})^{-1} = (z^{-1}x)^{-1}$
 $\Rightarrow zx^{-1} = x^{-1}z \Rightarrow x^{-1} \in C(R)$. \square

书后练习1.2. $P_{83}, Ex2$

证明： 任意 $a, b \in A$, $x \in R \Rightarrow xa \in I, xb \in I \Rightarrow (xa+xb) = x(a+b) \in I$
 $\Rightarrow a+b \in A$;

$xa \in I \Rightarrow -(xa) \in I \Rightarrow x(-a) \in I \Rightarrow -a \in A$;

任意 $a \in A$, $x, r \in R \Rightarrow (ra) \in I \Rightarrow x(ra) \in I \Rightarrow ra \in A$;

$$xa \in I \Rightarrow (xa)r \in I \Rightarrow x(ar) \in I \Rightarrow ar \in I;$$

所以 A 是 R 的理想;

再: 任意 $s \in I, x \in R \Rightarrow xs \in I \Rightarrow s \in A \Rightarrow I \subseteq A$. □

书后练习1.3. $P_{83}, Ex3$

证明: (1) $H + I$ 是子加群; 且任意 $x, y \in H + I$

\Rightarrow 存在 $h_1, h_2 \in H, s_1, s_2 \in I$, 使得: $x = h_1 + s_1, y = h_2 + s_2$

$\Rightarrow xy = (h_1 + s_1)(h_2 + s_2) = h_1h_2 + (s_1h_2 + h_1s_2 + s_1s_2) \in H + I$;

所以 $H + I$ 是 R 的子环;

I 显然是 $H + I$ 的子环, 且任意 $x \in H + I \subseteq R, s \in I \Rightarrow xs, sx \in I \Rightarrow I$ 是 $H + I$ 的理想;

两个子环的交仍是子环, 所以 $H \cap I$ 是 H 的子环.

再: 任意 $h \in H \subseteq R, s \in H \cap I \Rightarrow sh, hs \in H$ 且 $sh, hs \in I \Rightarrow sh, hs \in H \cap I$

$\Rightarrow H \cap I$ 是 H 的理想.

(2) 作 H 到 $(H + I)/I$ 的映射:

$$\begin{aligned}\phi: H &\rightarrow (H + I)/I \\ h &\mapsto h + I,\end{aligned}$$

ϕ 是 H 到 $(H + I)/I$ 的环同态, 且任意 $x + I \in (H + I)/I, x \in H + I$, 存在 $h \in H, s \in I$, 使得 $x = h + s \Rightarrow x + I = h + I \Rightarrow \phi(h) = h + I = x + I \Rightarrow \phi$ 是满同态;

$$x \in \text{Ker}\phi \Rightarrow x + I = 0 + I \Rightarrow x \in I \Rightarrow \text{Ker}\phi = H \cap I;$$

利用环的第一同态定理, 有:

$$H/(H \cap I) \cong (H + I)/I.$$

□

书后练习1.4. $P_{83}, Ex4$

证明: 作 R/I 到 R/J 的映射:

$$\begin{aligned}\phi: R/I &\rightarrow R/J \\ r + I &\mapsto r + J,\end{aligned}$$

(1) ϕ 是映射. $r_1 + I = r_2 + I \Rightarrow r_1 - r_2 \in I \subseteq J \Rightarrow r_1 + J = r_2 + J$;

(2) ϕ 保持运算. $r_1 + I, r_2 + I \in R/I$
 $\Rightarrow (r_1 + r_2) + I \mapsto (r_1 + r_2) + J = (r_1 + J) + (r_2 + J) = \phi(r_1 + I) + \phi(r_2 + I),$
 $\Rightarrow (r_1 r_2) + I \mapsto (r_1 r_2) + J = (r_1 + J) + (r_2 + J) = \phi(r_1 + I) + \phi(r_2 + I);$
 (3) ϕ 是满射. 任意 $r + J \in R/J$, 存在 $r + I \in R/I$, 使得 $\phi(r + I) = r + J;$
 (4) $\text{Ker}\phi = J/I.$

任意 $s + I \in J/I \subseteq R/J \Rightarrow s \in J \Rightarrow s + J = 0 + J \in R/J \Rightarrow s + I \in \text{Ker}\phi,$
 任意 $t + I \in \text{Ker}\phi \Rightarrow t + J = 0 + J \in R/J \Rightarrow t \in J \Rightarrow t + I \in J/I;$

利用环的第一同态定理, 有: $(R/I)/(J/I) \cong R/J.$ □

书后练习1.5. $P_{83}, Ex5$

证明: (1) $\text{Ker}\phi$ 是 R 的理想.

若 $\text{Ker}\phi = 0$, 结论成立;

若 $\text{Ker}\phi \neq 0$, 则存在 $0 \neq r \in \text{Ker}\phi \Rightarrow r^{-1}r = 1 \in \text{Ker}\phi$
 \Rightarrow 任意 $r \in R, r \cdot 1 = r \in \text{Ker}\phi \Rightarrow R \subseteq \text{Ker}\phi \Rightarrow \text{Ker}\phi = R.$

(2) \bar{R} 有单位元. 记 $\bar{1} = \phi(1) \in \bar{R}$, 任意 $\bar{r} \in \bar{R}$, 存在 $r \in R$, 使得
 $\phi(r) = \bar{r} \Rightarrow \begin{cases} \bar{r}\bar{1} = \phi(r)\phi(1) = \phi(r \cdot 1) = \phi(r) = \bar{r}, \\ \bar{1}\bar{r} = \phi(1)\phi(r) = \phi(1 \cdot r) = \phi(r) = \bar{r} \end{cases} \Rightarrow \bar{1} \text{ 是 } \bar{R} \text{ 的单位元};$

\bar{R} 是交换环. 任意 $\bar{a}, \bar{b} \in \bar{R}$, 存在 $a, b \in R$, 使得 $\phi(a) = \bar{a}, \phi(b) = \bar{b}$
 $\Rightarrow \bar{a}\bar{b} = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = \bar{b}\bar{a};$

\bar{R} 中每一个非 0 元都有逆元. 任意 $\bar{0} \neq \bar{a} \in \bar{R}$, 存在 $a \in R$, 使得
 $\phi(a) = \bar{a}, \phi$ 是同构 $\Rightarrow a \neq 0$, 又 R 是域 \Rightarrow 存在 $b \in R$, 使得 $ab = ba = 1$
 $\Rightarrow \phi(ab) = \phi(ba) = \phi(1) = \bar{1}. \phi(a)\phi(b) = \phi(b)\phi(a) = \bar{1} \Rightarrow \phi(b)$ 是 \bar{a} 在 \bar{R} 中的逆元. □

书后练习1.6. $P_{83}, Ex6$

证明: 记 \mathbb{Z}_m 中的元素为 \bar{s} , \mathbb{Z}_r 中的元素为 $[t]$. 这时,

$$\begin{aligned} \phi: \mathbb{Z}_m &\rightarrow \mathbb{Z}_r \\ \bar{a} &\mapsto [a], \end{aligned}$$

(1) ϕ 是映射. $\bar{a}_1 = \bar{a}_2 \Rightarrow m \mid (a_1 - a_2) \Rightarrow r \mid (a_1 - a_2) \Rightarrow [a_1] = [a_2];$

(2) ϕ 保持运算. $\bar{a}_1 + \bar{a}_2 = \overline{a_1 + a_2} \mapsto [a_1 + a_2] = [a_1] + [a_2];$

$\overline{a_1 a_2} = \overline{a_1} \overline{a_2} \mapsto [a_1 a_2] = [a_1][a_2].$

所以 ϕ 是 \mathbb{Z}_m 到 \mathbb{Z}_r 的群同态.

任意 $\bar{x} \in \text{Ker}\phi \Rightarrow [x] = [0] \Rightarrow r \mid x \Rightarrow \text{Ker}\phi = \{\bar{0}, \bar{r}, \dots, (\frac{m}{r}-1)\bar{r}\},$

$\mathbb{Z}_m/\text{Ker}\phi = \{\text{Ker}\phi, \bar{1} + \text{Ker}\phi, \dots, \overline{r-1} + \text{Ker}\phi\}.$ \square

§2 环的构造

书后练习2.1. $P_{91}, Ex1$

证明: 设 a 为环 R 的一个左零因子, 则存在 $0 \neq b \in R$, 使得 $ab = 0$.

若 $ba = 0$, 则 a 既是左零因子又是右零因子;

若 $ba \neq 0$, 记 $x = ba$, 则 $ax = a(ba) = (ab)a = 0$; $xb = (ba)b = b(ab) = 0$, x 既是左零因子又是右零因子. \square

书后练习2.2. $P_{91}, Ex2$

证明: 任意 $a_1 + b_1\sqrt{-5}, a_2 + b_2\sqrt{-5}, a_3 + b_3\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$,
 $a_i, b_i \in \mathbb{Z}, i = 1, 2, 3$, 则:

$(a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, $+$ 是 $\mathbb{Z}[\sqrt{-5}]$ 的代数运算;

$[(a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5})] + (a_3 + b_3\sqrt{-5})$
 $= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{-5}$
 $= (a_1 + b_1\sqrt{-5}) + [(a_2 + b_2\sqrt{-5}) + (a_3 + b_3\sqrt{-5})],$
 $(\mathbb{Z}[\sqrt{-5}], +)$ 满足结合律;

存在 $0 = 0 + 0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, $(a_1 + b_1\sqrt{-5}) + (0 + 0\sqrt{-5})$
 $= a_1 + b_1\sqrt{-5}$, $0 + 0\sqrt{-5}$ 是 $(\mathbb{Z}[\sqrt{-5}], +)$ 的单位元;

存在 $(-a_1) + (-b_1)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$,
 $(a_1 + b_1\sqrt{-5}) + [(-a_1) + (-b_1)\sqrt{-5}] = 0$, $(-a_1) + (-b_1)\sqrt{-5}$ 是 $a_1 + b_1\sqrt{-5}$ 的负元;

$(a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-5}$
 $= (a_2 + b_2\sqrt{-5}) + (a_1 + b_1\sqrt{-5})$, $(\mathbb{Z}[\sqrt{-5}], +)$ 满足交换律;

$(\mathbb{Z}[\sqrt{-5}], +)$ 是一个加群;

$(a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}) = (a_1a_2 - 5b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, \cdot 是 $\mathbb{Z}[\sqrt{-5}]$ 的代数运算;

$$\begin{aligned} & [(a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5})] \cdot (a_3 + b_3\sqrt{-5}) \\ &= [(a_1a_2 - 5b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-5}] \cdot (a_3 + b_3\sqrt{-5}) \\ &= [(a_1a_2 - 5b_1b_2)a_3 - 5(a_1b_2 + a_2b_1)b_3] + [(a_1a_2 - 5b_1b_2)b_3 + (a_1b_2 + a_2b_1)a_3]\sqrt{-5} \\ &= (a_1 + b_1\sqrt{-5}) \cdot [(a_2 + b_2\sqrt{-5}) \cdot (a_3 + b_3\sqrt{-5})], \end{aligned}$$

$(\mathbb{Z}[\sqrt{-5}], \cdot)$ 满足结合律;

$$\begin{aligned} & [(a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5})] \cdot (a_3 + b_3\sqrt{-5}) \\ &= (a_1 + b_1\sqrt{-5}) \cdot (a_3 + b_3\sqrt{-5}) + (a_2 + b_2\sqrt{-5}) \cdot (a_3 + b_3\sqrt{-5}), \\ & (a_3 + b_3\sqrt{-5}) \cdot [(a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5})] \\ &= (a_3 + b_3\sqrt{-5}) \cdot (a_1 + b_1\sqrt{-5}) + (a_3 + b_3\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}), \end{aligned}$$

乘法 \cdot 对加法 $+$ 有分配律;

$$1 = 1 + 0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}],$$

$1 \cdot (a_1 + b_1\sqrt{-5}) = a_1 + b_1\sqrt{-5} = (a_1 + b_1\sqrt{-5}) \cdot 1$, 1 是 $(\mathbb{Z}[\sqrt{-5}], \cdot)$ 的单位元;

$$(a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}) = (a_2 + b_2\sqrt{-5}) \cdot (a_1 + b_1\sqrt{-5}),$$

$(\mathbb{Z}[\sqrt{-5}], \cdot)$ 满足交换律;

$$\begin{aligned} & \text{若 } (a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}) = (a_1a_2 - 5b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-5} = 0 \\ & \text{且 } a_1 + b_1\sqrt{-5} \neq 0 \Rightarrow \begin{cases} a_1a_2 - 5b_1b_2 = 0 \\ a_1b_2 + a_2b_1 = 0 \end{cases} \end{aligned}$$

$$\begin{aligned} & \text{若 } a_1 \neq 0 \Rightarrow \begin{cases} a_2 = \frac{5b_1b_2}{a_1} \\ a_1b_2 + a_2b_1 = 0 \end{cases} \Rightarrow a_1b_2 + \frac{5b_1b_2}{a_1}b_1 = 0 \\ & \Rightarrow (a_1^2 + 5b_1^2)b_2 = 0 \Rightarrow b_2 = 0 \Rightarrow a_2 = 0 \\ & \Rightarrow a_2 + b_2\sqrt{-5} = 0; \end{aligned}$$

$$\begin{aligned} & \text{若 } b_1 \neq 0 \Rightarrow \begin{cases} b_2 = \frac{a_1a_2}{5b_1} \\ a_1b_2 + a_2b_1 = 0 \end{cases} \Rightarrow (a_1^2 + 5b_1^2)a_2 = 0 \Rightarrow a_2 = 0 \Rightarrow \\ & b_2 = 0 \\ & \Rightarrow a_2 + b_2\sqrt{-5} = 0; \end{aligned}$$

所以 $(\mathbb{Z}, +, \cdot)$ 是有单位元且没有零因子的交换环, 是整环. \square

书后练习2.3. $P_{91}, Ex3$

证明: 在实连续函数环 $C[0, 1]$ 中, 存在函数

$$f(x) = \begin{cases} 0 & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} & \frac{1}{2} < x \leq 1 \end{cases}; g(x) = \begin{cases} x - \frac{1}{2} & 0 \leq x \leq \frac{1}{2} \\ 0 & \frac{1}{2} < x \leq 1 \end{cases}$$

满足: $f(x) \neq 0, g(x) \neq 0$ 但 $f(x)g(x) = 0$, 亦即 $C[0, 1]$ 中存在零因子. 所以 $C[0, 1]$ 不是整环;

在 n 是合数时, 设 $n = n_1 n_2, n_1 < n, n_2 < n$, 则 $[n_1] \neq 0, [n_2] \neq 0$ 而 $[n_1][n_2] = [n_1 n_2] = [n] = 0$, 所以 \mathbb{Z}_n 不是整环. \square

书后练习2.4. $P_{92}, Ex4$

解: $\mathbb{Z}[i] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ 它是一个整环.

$\mathbb{Z}[i]$ 的分式域

$$\begin{aligned} \overline{\mathbb{Z}[i]} &= \{\alpha\beta^{-1} \mid \alpha, \beta \in \mathbb{Z}[i], \beta \neq 0\} \\ &= \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\} \\ &= \mathbb{Q}[\sqrt{-1}]. \end{aligned}$$

\square

书后练习2.5. $P_{92}, Ex5$

证明: F_n 是域 F 上的所有 n 阶方阵的全体.

F_n 关于矩阵的加法和乘法构成一个环;

F_n 关于矩阵的加法和 F 与 F_n 的纯量乘法构成一个维数不大于 n^2 的线性空间;

所以 F_n 是域 F 上的一个有限维代数. \square

§3 多项式环

书后练习3.1. $P_{98}, Ex1$

解: \mathbb{Z}_7 是一个域. 利用分配律

$$\begin{aligned} &([3]x^2 + [5]x + [4])([4]x^2 + [2]x + [3]) \\ &= [12]x^4 + [6]x^3 + [9]x^2 + [20]x^3 + [10]x^2 + [15]x + [16]x^2 + [8]x + [12] \\ &= [5]x^4 + [5]x^3 + [2]x + [5]. \end{aligned}$$

\square

书后练习3.2. $P_{98}, Ex2$

解: (1) $(x+i)(x-i) = x^2 - ix + ix - i \cdot i = x^2 + 1$;

(2) 在 $x = k$ 时, $x^2 + 1 = k^2 + 1 = (-1) + 1 = 0$, 而

$$(k+i)(k-i) = k^2 - ki + ik - ii = j + j \neq 0.$$

□

书后练习3.3. $P_{98}, Ex3$

证明: R 中有单位元 1, 且 $1 \in R[x]$ 也是 $R[x]$ 的单位元;

任意 $a_0 + a_1x + \dots + a_nx^n, b_0 + b_1x + \dots + b_mx^m \in R[x]$, 有:

$$\begin{aligned} & (a_0 + a_1x + \dots + a_nx^n) \cdot (b_0 + b_1x + \dots + b_mx^m) \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)x + \dots + \left(\sum_{i=0}^k a_ib_{k-i}\right)x^k + \dots + a_nb_mx^{n+m} \\ &= (b_0a_0) + (b_1a_0 + b_0a_1)x + \dots + \left(\sum_{i=0}^k b_{k-i}a_i\right)x^k + \dots + a_nb_mx^{n+m} \\ &= (b_0 + b_1x + \dots + b_mx^m) \cdot (a_0 + a_1x + \dots + a_nx^n), \text{ 其中 } i > n \text{ 时 } a_i = 0, k-i > m \\ & \text{ 时 } b_{k-i} = 0. \end{aligned}$$

$R[x]$ 满足交换律;

任意 $0 \neq a_0 + a_1x + \dots + a_nx^n, 0 \neq b_0 + b_1x + \dots + b_mx^m \in R[x]$, 不妨设 $a_n \neq 0, b_m \neq 0$, 则

$$\begin{aligned} & (a_0 + a_1x + \dots + a_nx^n) \cdot (b_0 + b_1x + \dots + b_mx^m) \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)x + \dots + \left(\sum_{i=0}^k a_ib_{k-i}\right)x^k + \dots + a_nb_mx^{n+m} \neq 0, \end{aligned}$$

$R[x]$ 中没有零因子;

所以 $R[x]$ 是整环.

□

书后练习3.4. $P_{98}, Ex4$

证明: (1) $T \neq \emptyset$, 且任意 $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in T$, 有

$$\begin{aligned} \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} &= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & c_1 + c_2 \end{pmatrix} \in T, \\ -\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} &= \begin{pmatrix} -a_1 & -b_1 \\ 0 & -c_1 \end{pmatrix}, \end{aligned}$$

$(T, +)$ 是 $(M_2(\mathbb{Z}), +)$ 的子加群;

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in T,$$

(T, \cdot) 是封闭的;

所以 $(T, +, \cdot)$ 是 $(M_2(\mathbb{Z}), +, \cdot)$ 的子环.

(2) 直接验证: $(I, +)$ 是 $(M_2(\mathbb{Z}), +)$ 的子加群;

任意 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T$, $\begin{pmatrix} 0 & 2d \\ 0 & 0 \end{pmatrix} \in I$, 有

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & 2d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2ad \\ 0 & 0 \end{pmatrix} \in I, \quad \begin{pmatrix} 0 & 2d \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & 2cd \\ 0 & 0 \end{pmatrix} \in I,$$

所有 I 是 T 的理想;

注: I 不是 $(M_2(\mathbb{Z}), +)$ 的理想.

(3) 记 T/I 中的元素为 $\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right]$, 则

$$\left[\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \right] = \left[\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \right] \Leftrightarrow \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in I$$

$$\Leftrightarrow \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in I \Leftrightarrow \begin{cases} a_1 = a_2 \\ c_1 = c_2 \\ b_1 - b_2 \in 2\mathbb{Z} \end{cases}, \text{ 所以}$$

$$T/I = \left\{ \left[\begin{pmatrix} x & 1 \\ 0 & y \end{pmatrix} \right], \left[\begin{pmatrix} x & 2 \\ 0 & y \end{pmatrix} \right] \mid x, y \in \mathbb{Z} \right\}.$$

□

书后练习3.5. $P_{08}, Ex5$

证明: (1) $I_n \in D(R)$, $D(R) \neq \emptyset$; 且

$$D(R) + D(R) = D(R), \quad -D(R) = D(R), \quad D(R) \cdot D(R) = D(R),$$

所以 $D(R)$ 是 $M_n(R)$ 的子环;

(2) 因为 R 是交换环, 所以 $D(R) \subseteq C(D(R))$;

记 E_i 是 (i, i) 位置为 1, 其余位置为 0 的 n 阶方阵, 则 $E_{ii} \in D(R)$,
再: 任意 $A = (a_{ij})_n \in C(D(R))$, 则

$$E_i A = A E_i,$$

亦即

$$\begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} \\ 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & a_{ii} & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}$$

$\Rightarrow i \neq j, a_{ij} = 0 \Rightarrow A \in D(R),$

所以 $C(D(R)) = D(R).$

□

§4 交换环

书后练习4.1. $P_{104}, Ex1$

证明: (1) 环 R 的特征为 $p \Rightarrow$ 任意 $r \in R$ 有 $pr = 0.$

再: R 是交换环, 在交换环中牛顿二项式定理成立, 所以

$$(a+b)^{p^n} = \sum_{k=0}^{p^n} C_{p^n}^k a^k b^{p^n-k},$$

注意到: $0 < k < p^n$ 时, $p \mid C_{p^n}^k \Rightarrow C_{p^n}^k a = 0,$

所以

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

(2) ϕ 是 R 上的映射. 且

$$\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b),$$

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b),$$

ϕ 是 R 到 R 的环同态.

(3) 要证明: ϕ 是 R 上的一一对应.

$$\text{Ker}\phi = \{r \in R \mid r^p = 0\} = \{0\} \Rightarrow \phi \text{ 是单射};$$

任意 $a \in R,$

□

书后练习4.2. $P_{104}, Ex2$

证明: $\mathbb{Z}[i]$ 是有单位元 1 的交换环; 要证明 $\mathbb{Z}[i]/(1+i)$ 是域, 只要证明: $(1+i)$ 是 $\mathbb{Z}[i]$ 的极大理想.

由于 $\mathbb{Z}[i]$ 是有单位元的交换环, 所以

$$(1+i) = \{(a+bi)(1+i) \mid a+bi \in \mathbb{Z}[i]\}.$$

任取 $\mathbb{Z}[i]$ 的一个理想 $J \supsetneq (1+i)$, 则存在 $c+di \in J$ 且 $c+di \notin (1+i)$.

由于 $(1+i)(1+i) = -2i \in (1+i) \Rightarrow 2 = 2(1+i) - 2i \in (1+i) \Rightarrow 2k+2li, (2k+1) + (2l+1)i = (2k+2li) + (1+i) \in (1+i), \forall k, l \in \mathbb{Z} \Rightarrow c-d$ 是奇数.

再

$$c+di = 2k + (2l+1)i \Rightarrow i = 2k + (2l+1)i - (2k+2li) \in J;$$

$$c+di = (2k+1) + (2l)i \Rightarrow i = 2k + (2l+1)i - (2k+2li) \in J.$$

在 $i \in J$ 时, $-1 = ii \in J \Rightarrow 1 \in J$.

所以 $1 \in J \Rightarrow J = \mathbb{Z}[i] \Rightarrow (1+i)$ 是 $\mathbb{Z}[i]$ 的极大理想
 $\Rightarrow \mathbb{Z}[i]/(1+i)$ 是域. □

书后练习4.3. $P_{104}, Ex3$

证明: R 是没有单位元的交换环. 所以

$$(4) = \{2k \cdot 4 + n \cdot 4 \mid k, n \in \mathbb{Z}\} = \{\text{所有 } 4 \text{ 的倍数}\},$$

它是 R 的最大理想.

事实上: 取 R 的真理想 J , 如果 $J \subseteq (4)$, 则至少存在一个数 $n = 4k+2 \in J$ 且 $n \notin (4)$. 从而 $2 \in J \Rightarrow J = R$.

$2 \notin (4)$, 所以在 $R/(4)$ 中, $\bar{2} = 2+(4) \neq \bar{0}$, 而 $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$, 亦即: $R/(4)$ 中有零因子. 所以 $R/(4)$ 不是域. □

书后练习4.4. $P_{104}, Ex4$

证明: $\mathbb{Z}[i]$ 是有单位元的交换环, 所以

$$(5) = \{5(a+bi) \mid a+bi \in \mathbb{Z}[i]\} = \{5a+5bi \mid a, b \in \mathbb{Z}\},$$

$$(11) = \{11(a+bi) \mid a+bi \in \mathbb{Z}[i]\} = \{11a+11bi \mid a, b \in \mathbb{Z}\}.$$

(1) $1+2i \notin (5), 1-2i \notin (5)$ 但 $(1+2i)(1-2i) = 5 \in (5)$,
所以 (5) 不是素理想;

(2) 任意 $a+bi \notin (11)$, 则

$$11 \nmid a, 11 \nmid b \text{ 或者 } 11 \mid a, 11 \nmid b \text{ 或者 } 11 \nmid a, 11 \nmid b,$$

取 $x + yi \in \mathbb{Z}[i]$, 使得

$$(x + yi)(a + bi) = (ax - by) + (bx + ay)i \in (11),$$

亦即:

$$\begin{cases} 11 \mid (ax - by) \\ 11 \mid (bx + ay) \end{cases}$$

$$\Rightarrow \begin{cases} ax - by = 11n \\ bx + ay = 11m \end{cases} \quad m, n \in \mathbb{Z}$$

$$\Rightarrow \begin{cases} (a^2 + b^2)x = 11(an + bm) \\ (a^2 + b^2)y = 11(am - bm) \end{cases},$$

在 $11 \nmid a$, $11 \mid b$ 或者 $11 \mid a$, $11 \nmid b$ 时, 有 $11 \nmid (a^2 + b^2)$, 从而

$$11 \mid x \text{ 且 } 11 \mid y,$$

$$x + yi \in (11);$$

在 $11 \nmid a$, $11 \nmid b$ 时, 设

$$\begin{cases} a = 11k + r_1, & 0 < r_1 < 11 \\ b = 11l + r_2, & 0 < r_2 < 11 \end{cases}$$

则

$$a^2 + b^2 = 11s + r_1^2 + r_2^2$$

由下列的加法表:

+		1	4	9	16	25	36	49	64	91	100
-		-	-	-	-	-	-	-	-	-	-
1		2									
4		5	8								
9		10	13	18							
16		17	20	25	32						
25		26	29	34	41	50					
36		37	40	45	52	61	72				
49		50	53	58	65	74	85	98			
64		65	68	73	80	89	100	113	128		
81		82	85	90	97	106	117	130	145	162	
100		101	104	109	116	125	136	149	164	181	200

可以得到: $11 \nmid (r_1^2 + r_2^2)$, 亦即: $11 \nmid (a^2 + b^2)$, 所以

$$11 \mid x \text{ 且 } 11 \mid y,$$

所以 $x + yi \in (11)$. (11) 是 $\mathbb{Z}[i]$ 的素理想.

书后练习4.5. P_{104} , Ex5

证明: 显然 $\bigcap_{i=1}^{\infty} P_i = P \neq R$.

任意 $x, y \in R$, 满足 $x \cdot y \in P$ 且 $x \notin P$, 要证明: $y \in P$.

假设 $y \notin P$, 则存在 m , 使得 $y \notin P_m$. 又 $x \notin P$, 所以存在 n , 使得 $y \notin P_n$, 取 $t = \min\{m, n\}$, 由于 $P_m \supseteq P_t, P_n \supseteq P_t$, 从而 $x \notin P_t$ 且 $y \notin P_t$. 再: P_t 是素理想, 所以 $x \cdot y \notin P_t$, 从而 $x \cdot y \notin P$, 矛盾. 所以 P 仍是素理想. \square

§5 整环的整除理论

书后练习5.1. P_{115} , Ex1

证明: (1) 假设 $a + bi$ 是单位, 则存在 $c + di \in \mathbb{Z}[i]$, 使得

$$(a + bi)(c + di) = 1,$$

而 $N((a + bi)(c + di)) = N(a + bi)N(c + di)$, 所以 $N(a + bi) = N(c + di) = 1$.

假设 $a + bi \in \mathbb{Z}[i]$, 满足: $N(a + bi) = a^2 + b^2 = 1$, 所以 $a = \pm 1, b = 0$ 或者 $a = 0, b = \pm 1$, 即 $a + bi = 1, a + bi = -1, a + bi = i, a + bi = -i$.

而 $1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i) = (-i) \cdot i = 1$, 所以 $\pm 1, \pm i$ 是 $\mathbb{Z}[i]$ 的单位.

(2) 设 $\alpha = a + bi$ 是 $1 - 2i$ 的因子, 则存在 $\beta = c + di \in \mathbb{Z}[i]$, 使得

$$1 - 2i = (a + bi)(c + di),$$

从而 $N(1 - 2i) = N((a + bi)(c + di)) = N(a + bi)N(c + di)$, 即 $N(a + bi)N(c + di) = 5$. 由于 5 是素数, 所以 $N(a + bi) = 5, N(c + di) = 1$ 或者 $N(a + bi) = 1, N(c + di) = 5$.

利用 (1) 的结论, 有 $c + di$ 为单位或者 $a + bi$ 是单位, 所以 $1 - 2i$ 的因子只有单位以及 $1 - 2i$ 的相伴元. 所以 $1 - 2i$ 是 $\mathbb{Z}[i]$ 中的既约元. \square

书后练习5.2. $P_{116}, Ex2$

证明: 要证明: $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ 是 Euclid 环, 关键是找到 $\mathbb{Z}[\sqrt{2}]$ 到 $\{0\} \cup \mathbb{Z}^+$ 的映射 ϕ , 使得任意 $x, y \in \mathbb{Z}[\sqrt{2}], y \neq 0$, 都存在 $q, r \in \mathbb{Z}[\sqrt{2}]$, 使得 $x = qy + r$, 其中 $r = 0$ 或者 $\phi(r) < \phi(y)$.

在 $\mathbb{Z}[\sqrt{2}]$ 上定义映射:

$$\begin{aligned}\phi: \mathbb{Z}[\sqrt{2}] &\rightarrow \{0\} \cup \mathbb{Z}^+ \\ a + b\sqrt{2} &\mapsto N(a + b\sqrt{2}) = |a^2 - 2b^2|,\end{aligned}$$

下面验证: 任意 $x, y \in \mathbb{Z}[\sqrt{2}]$, 满足

$$N(xy) = N(x)N(y).$$

设 $x = a + b\sqrt{2}, y = c + d\sqrt{2}$, 则 $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$
 $\Rightarrow N(xy) = |(ac + 2bd)^2 - 2(ad + bc)^2| = |(a^2 - 2b^2)(c^2 - 2d^2)| = N(x)N(y).$

对任意的 $\alpha = a + b\sqrt{2}, \beta = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \beta \neq 0$, 现在我们在 $\mathbb{Z}[\sqrt{2}]$ 的商域 $\mathbb{Q}\sqrt{2}$ 上考虑 $\frac{\alpha}{\beta}$, 可设 $\frac{\alpha}{\beta} = x + y\sqrt{2}, x, y \in \mathbb{Q}$.

由于 $x, y \in \mathbb{Q}$, 所以存在 $u, v \in \mathbb{Z}$, 使得 $|x - u| \leq \frac{1}{2}, |y - v| \leq \frac{1}{2}$,
 取 $q = u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \frac{\gamma}{\beta} = (x - u) + (y - v)\sqrt{2}$,
 则 $N(\frac{\gamma}{\beta}) = |(x - u)^2 - 2(y - v)^2| \leq |(x - u)^2| + 2|(y - v)^2| \leq \frac{1}{4} + 2\frac{1}{4} < 1.$

这样, 存在 $q = u + v\sqrt{2}$,
 $\gamma = [(x - u) + (y - v)\sqrt{2}](c + d\sqrt{2}) = (x + y\sqrt{2})(c + d\sqrt{2}) - (u + v\sqrt{2})(c + d\sqrt{2})$
 $= (a + b\sqrt{2}) - (u + v\sqrt{2})(c + d\sqrt{2}) \in \mathbb{Z}[\sqrt{2}],$ 满足:
 $\alpha = q\beta + \gamma, N(\gamma) < N(\beta),$
 所以 $\mathbb{Z}[\sqrt{2}]$ 是 Euclid 环. □

书后练习5.3. $P_{116}, Ex3$

证明: 设 R 是 Euclid 环, I 是 R 的一个非零理想.

由于 R 上存在一个映射:

$$\phi: \{R \text{ 的非零元全体} \} \rightarrow \mathbb{Z}^+ \cup \{0\};$$

则 $\phi(I - \{0\})$ 是一个非空自然数集, 那么存在最小自然数 $m \in \phi(I - \{0\})$.
 从而存在 $a \in R, a \neq 0$, 使得 $\phi(a) = m$.

任意 $b \in I$, 由于 R 是 Euclid 整环, 所以存在 $q, r \in R$, 使得

$$b = aq + r, \text{ 其中 } r = 0 \text{ 或 } \phi(r) < \phi(a).$$

又 $a, b \in I$, 所以 $r = b - aq \in I$, 再, $\phi(a)$ 是 $\phi(I - \{0\})$ 的最小元, 所以 $r = 0$, 从而 $b = aq \in (a) \Rightarrow I = (a)$. \square

书后练习5.4. $P_{116}, Ex4$

证明: 设 R 是一个主理想整环, I 是其任意理想, $I = (a)$. 考虑自然环同态:

$$\begin{aligned}\phi: R &\rightarrow R/I \\ r &\mapsto [r] = r + I,\end{aligned}$$

任取 R/I 的一个理想 J' , 其在 ϕ 之下的完全原象为 $\phi^{-1}(J') = J$, 则 $J \supseteq I$ 是 R 的理想. 由 R 是主理想整环, 所以可设 $J = (b) = Rb = \{rb \mid r \in R\}$, 如下要证明: $J' = ([b])$.

因为 $b \in J$, 所以 $[b] \in J'$, 任意 $[c] \in J'$, 则存在 $c \in J$ 使得 $\phi(c) = [c]$. 又 $J = (b)$, 所以存在 $r \in R$ 使得 $c = rb$, 所以 $[c] = \phi(c) = \phi(rb) = \phi(r)\phi(b) = [r][b] \in ([b])$. 所以 $J' \subseteq ([b])$, 又 $[b] \in J'$, $([b]) \subseteq J'$, 所以 $J' = ([b])$. \square

书后练习5.5. $P_{116}, Ex5$

证明: R 是唯一分解环, 所以 R 是一个整环. 且任意 $a \in R$, 存在唯一的既约元标准分解:

$$a = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}, \quad p_i \text{ 是 } R \text{ 中的不相伴的素元, } r_i \text{ 是正整数.}$$

对任意的元素 $a, b \in R$, 设它们的标准分解分别为:

$$a = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}, \quad b = q_1^{n_1} q_2^{n_2} \cdots q_t^{n_t},$$

取 a, b 的标准分解式中相伴的既约元因子, 由于 R 是交换环, 不妨设 p_1 与 q_1 相伴, \dots , p_m 与 q_m 相伴. 记

$$c = p_1^{\min\{r_1, n_1\}} p_2^{\min\{r_2, n_2\}} \cdots p_m^{\min\{r_m, n_m\}},$$

下面证明: c 是 a, b 的最大公因子.

首先 c 是 a, b 的公因子;

假设 d 是 a, b 的公因子, d 的分解式为:

$$d = u_1^{s_1} u_2^{s_2} \cdots u_v^{s_v}$$

由 $d \mid a$, 可知 u_i 是 a 的既约因子, 也是 b 的既约因子, 再由消去律, s_i 不会超过它们在 a, b 的标准分解式中的指数, 所以 $d \mid c$, 也就是: c 是 a, b 的最

大公因子.

□

书后练习5.6. $P_{116}, Ex6$

证明: 因为 $a \in (b) \Leftrightarrow b \mid a$, 且 $(b) = (c) \Leftrightarrow b$ 与 c 相伴, 又因为 R 是唯一分解环, 所以任意 $0 \neq a \in R$, a 的真因子是有限的, 所以 R 中仅有有限个含 a 的主理想.

□

§6 环的表示与模